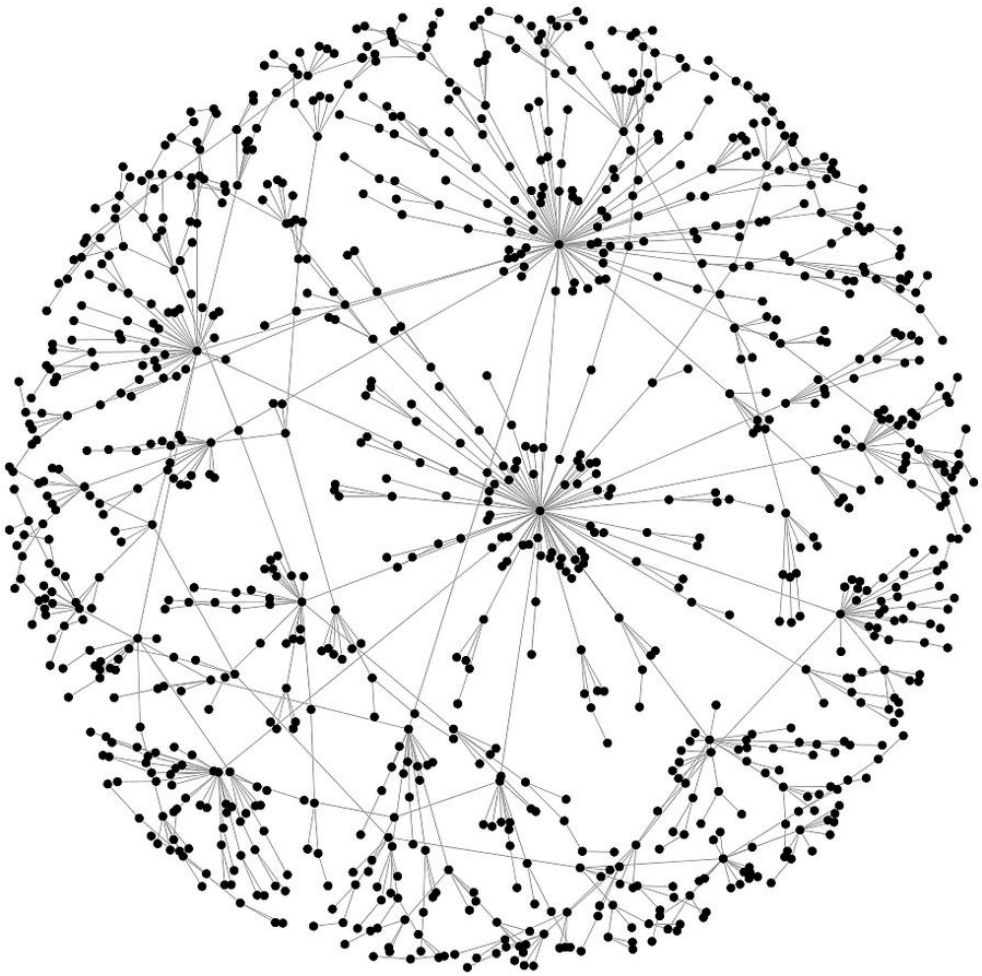
CYBERATTACK-RELATED CASCADING EFFECTS MITIGATION

A RISK-BASED APPROACH FOR ICS NETWORK SEGMENTATION DESIGN IN CHEMICAL PLANTS

RADITYA ARIEF



TU Delft

This page intentionally left blank

Cyberattack-Related Cascading Effects Mitigation

A Risk-Based Approach for ICS Network Segmentation Design in Chemical Plants

---

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

Raditya Arief

Student number: 4500318

To be defended in public on November 29th, 2018

Graduation committee

Chairperson	:	Prof.dr.ir. G.L.L. Reniers, Section Safety and Security Science
First Supervisor	:	Dr.ir. N. Khakzad, Section Safety and Security Science
Second Supervisor	:	Dr.ir. G.A. de Reuver, Section Information and Communication Technology
Third Supervisor	:	Dr.ir. W. Pieters, Section Safety and Security Science

This page intentionally left blank

Preface

The completion of this thesis report concluded an important chapter of my life. Through this journey, I have learned to deal with problems in a structured and methodical manner, to be critical of ideas, and to be mindful and questioned every assumption. More than anything, the whole process has attested that hard work, perseverance, and prayers will always bring you a step closer toward your goal.

Nevertheless, I would not have arrived at this point without the help and support given to me. Hence, it is my pleasure for me to express my heartfelt gratitude to those who have made the completion of this thesis possible. First of all, I would like to extend my utmost gratitude to my first supervisor, Nima, whose constant guidance have deeply shaped this thesis. Through our discussions and his remarkably meticulous feedback, he has shown his passion for the subject which has motivated me to continuously improve the quality of this work. I would also like to thank Mark, with whom I did my master's thesis preparation with, for willingly join the committee at the very last stage to help me proceed and finish this thesis. My thank also goes to Wolter, not only for helping me at the beginning to discover this topic and to acquaint me with Nima, but also for willingly offer his guidance to the very end. Finally, I would like to thank Prof. Genserik Reniers whose insight and feedback have ensured the scientific quality and the practical relevance of this thesis.

Also, I would like to extend my gratitude to my families and friends. To my fellow Indonesian friends in Delft, whom I can always count on to bring the warmth and comfort of home. My parents, whose endless yet unconditional support has been the cornerstone of all my endeavor. Last but foremost, to the love of my life, Stefanie, with whom I have shared the struggle over the entirety of this period. To know that she will always be waiting at the finish line has always been the source of my strength.

Raditya Arief

Delft, 2018

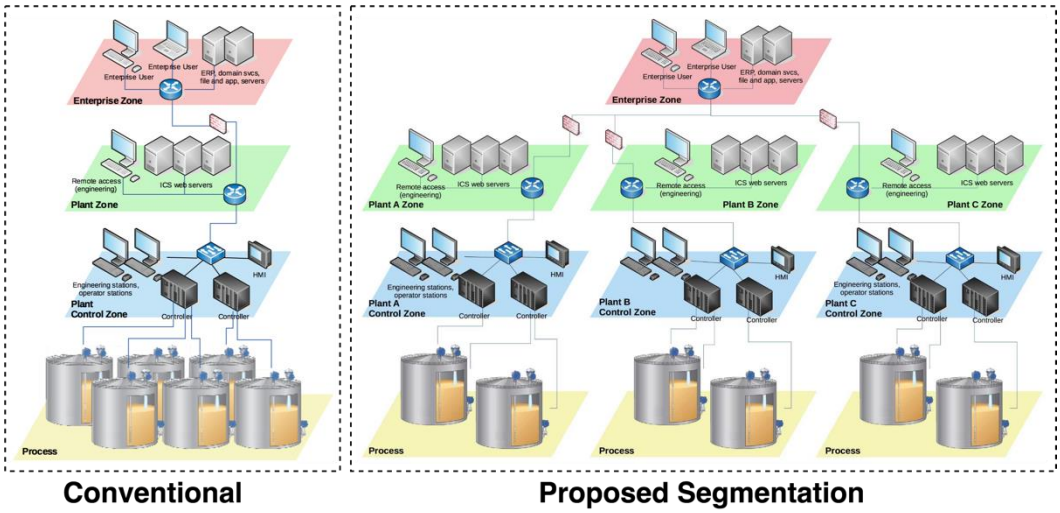
This page intentionally left blank

Executive Summary

Cascading effects in chemical and process plants are phenomena where single or multiple accidents propagate throughout the system. Cascading effects are primarily driven by the interdependency and interconnectivity of components within the plants. Moreover, the majority of industrial facilities and critical infrastructures in general, and chemical and process plants in particular, have adopted Industrial Control Systems (ICSs) to improve the management of their operation. However, despite their apparent benefits, the adoption of ICSs by the industry has invited some criticisms due to its vulnerability against cyberattacks. This development has not only introduced various cyber-vulnerabilities that did not previously exist but has also expanded the threat landscape of this equipment.

One of the impacts of the development mentioned above of ICSs in chemical and process plants is the emergence of the risk of cyberattack-related cascading effects. This concern can be corroborated by several factors, such as the increasing trend of successful cyberattacks toward industrial facilities (Lee et al., 2014; Sanger, 2012), indications that intentional attacks are the potential cause for cascading effects (Boyes, 2013; Crucitti et al., 2004; Wang et al., 2014; Zhao et al., 2004), and the indicated presence of threat actors that are motivated to exploit these vulnerabilities. All in all, these factors strongly indicate the risk of cyberattack-related cascading effects.

To mitigate the risk of cyberattack-related cascading effects, this master's thesis proposes the utilization of ICS network segmentation in chemical and process plants. ICS network segmentation is defined as the practice of partitioning an ICS network architecture into multiple smaller segments, and it is already regarded as a common approach used by businesses and organizations to improve their cybersecurity. An example of an ICS network segmentation in a tank farm is presented in the following Figure.

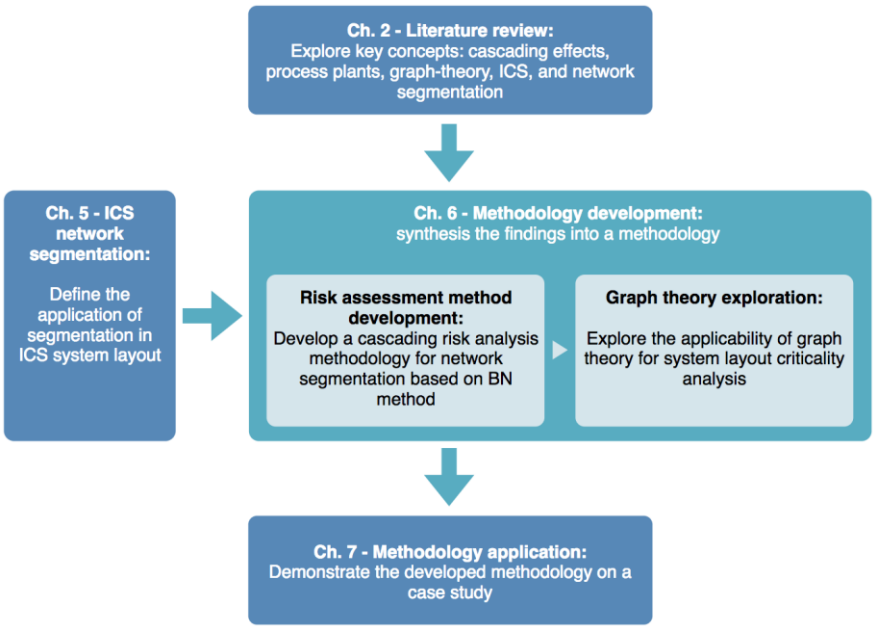


To utilize network segmentation to mitigate cyberattack-related cascading effects risk, a risk-based approach is adopted for this thesis. In a risk-based approach, the decisions regarding the design are chosen according to the risk being. Accordingly, the objective of this thesis is to develop a risk-based methodology for developing ICS network segmentation in chemical and process plants that will improve the systems' robustness against cyberattack-related cascading effects. Based on the

research objective and the research background, the main research question for this study is formulated as follow:

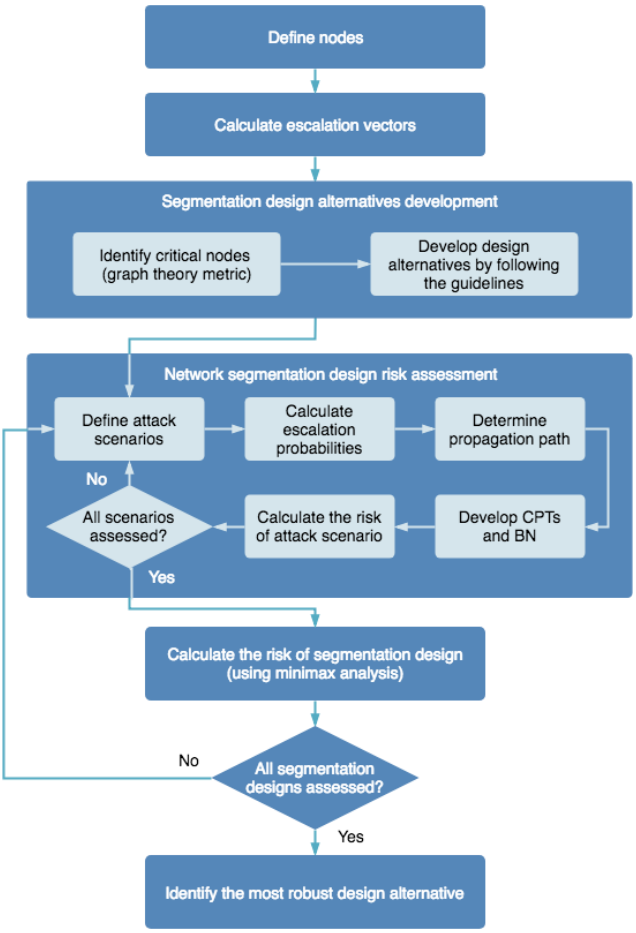
> **Main Research Question** – How to optimize ICS network segmentation design in chemical plants to improve its robustness against cascading effects under cyberattacks?

Several steps must be followed to answer the main research question. For this purpose, a research framework is developed to outline the strategies and the flow used in achieving the goal of this thesis. The figure exhibits the research flow diagram of this thesis, depicting the activities pursued in this thesis, how they relate to each other, and the corresponding methods used to fulfill them.



The first step is to gain comprehension about the implication of network segmentation to cyberattack-related cascading effects. For that purpose, explorations and research to some more fundamental aspects are required, such as the implementation of network segmentation in ICSs, the process of cyberattacks on ICSs, the implication of network segmentation to cyberattacks, and others. To elicit some insights on this matter, exploration to assorted sources are performed, such as from academic journals, whitepapers from ICS manufacturers, government reports, and others.

Once the implication of network segmentation to cyberattack-related cascading effects is understood, the next step is to calculate and analyze the risk of cyberattack-related cascading effects in chemical and process plants. Hence, a method to model and analyze cyberattack-related cascading effects which take into the effect of network segmentation into account must first be developed. For that purpose, a BN method for cascading effects modeling and analysis by Khakzad et al. (2013) is adopted. The BN method is used as the point of departure, and it is subsequently expanded to account for the implication of network segmentation. Ultimately, a risk-based method to analyze the risk of cyberattack-related cascading effects in various network segmentation designs is developed. The process flow of the risk-based methodology is presented in the figure below.



However, as already discovered during the preliminary literature review, the process of risk assessment using the BN method can be lengthy and complicated. To solve this problem, an additional process is incorporated into the segmentation design development stage, prior to the risk assessment stage. This thesis presents some design guidelines for developing robust networks segmentation designs. The main building block of the design guidelines is criticality analysis on the component level using graph theory metrics from the work of Khakzad and Reniers (2015). The graph theory approach enables early identification of the severity of cascading effects on network segmentation designs. Also, some other guidelines based on some insights obtained from the literature review are also provided. By incorporating these guidelines, it is expected that the segmentation design development stage would produce more robust design alternatives.

Finally, the risk-based method and the design guidelines are applied to a case study. This part of the thesis is devoted to demonstrating the application of the risk-based method, as well as to examine the efficacy of the method. In this case study, several network segmentation design alternatives are developed and evaluated: three design alternatives are developed by following the design guidelines (i.e., Network Design 1-3), one design is developed without the guidelines (Network Design 4), and for the sake of comparison, the robustness of a non-segmented network is also evaluated. The results from the case study are presented in the table below.

Comparing the risk analysis results, it can be seen that all the design alternatives developed by following the guidelines have higher robustness compared to the design developed without any guidelines. Moreover, the risk of cyberattack-related cascading effects in the non-segmented network design is higher than the other designs. Interestingly, the findings suggest that the application of network segmentation would reduce the risk of cyberattack-related cascading effects, even when the design is developed without the proposed guidelines. Nevertheless, the utilization of the design guidelines has been proven to improve the robustness of the network design further.

Design	Risk
Segmented design (with guidelines)	
Network Design 1	€ 28,133.07
Network Design 2	€ 29,774.78
Network Design 3	€ 28,031.03
Segmented design (without guidelines)	
Network Design 4	€ 38,647.28
Non-segmented (flat) design	
Non-segmented network design	€ 68,557.00

From this result, several contributions of this thesis can be outlined. From the scientific perspective, the present study attempts to fill a knowledge gap between cyberattacks and cascading effects in chemical and process plants. Moreover, the deliverables of this thesis can be described as follow:

- A risk evaluation method for cyberattack-related cascading effects
- Demonstration of the efficacy of network segmentation in reducing the risk of cyberattack-related cascading effects
- Identification of the design aspects of network segmentation that critical to its robustness against cyberattack-related cascading effects

The deliverables contribute to the body of knowledge of the related domains. Besides the main contribution, the risk evaluation method developed in this study also contributes to the attempt to quantify the impact of network segmentation.

From a practical standpoint, some insight and recommendations can be given to practitioners based on the result of this study. This study has demonstrated ICS network segmentation as an effective means in mitigating the risk of cyberattack-related cascading effects, and a methodology to develop an effective solution to improve the robustness of systems against the risk of cyberattack-related cascading effects has been offered. However, looking at the current trend, where businesses and organizations are likely to overlook the risk of high-impact, low probability events such as cascading effects due to its low probability, it seems unlikely that the finding presented in this thesis would change the current practice. On a side note, this study has also found that the implementation of network segmentation, regardless of the objectives, would reduce the risk of cyberattack-related cascading effects in case of an attack (albeit not as effective). Therefore, without disregarding the presence of trade-offs associated with the implementation of network segmentation, the result of this study contributes to the list of advantages offered by network segmentation.

Some limitations of the present study have also been identified. Firstly, the efficacy of the risk-based methodology and the design guidelines are dependent on the accuracy of the methods adopted in this study. Second, a knowledge gap relating to the connection between ICS components in chemical and process plants and potential accidents has been identified. The lack of understanding has hampered the attempt to bridge the result from cascading effects analysis and the network design. Lastly, there are several limitations that are associated with the utilization of game theory. From these drawbacks, and some improvement ideas, the following recommendations for future research are presented:

- To utilize a more sophisticated methods for the risk-based methodology (e.g., dynamic BN method in place of the conventional BN method)

- To conduct further research to foster an understanding of the relationship between ICS components and the potential accidents
- Use an alternative approach in place of game theory. For instance, agent-based modeling can be utilized to simulate the behavior of attackers
- Develop a method to determine the optimal number of segments of the network segmentation design
- Expand the risk assessment to include off-site risks as well as on-site risks
- Extend the risk assessment method to include the effects of add-on safety barriers (e.g., water deluge systems or fireproof coating)
- A more holistic analysis of network segmentation to understand the trade-offs of its implementation

This page intentionally left blank

Table of Content

This page intentionally left blank

List of Tables

List of Figures

List of Abbreviations

BN	Bayesian network
CI	Critical infrastructure
COTS	Commercial off-the-shelf
CPT	Conditional probability table
DCS	Distributed control system
DHS	Department of Homeland Security
DMZ	Demilitarized zone
HILP	High-impact, low-probability
HMI	Human machine interface
ICS	Industrial control systems
ICS–CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and communication technologies
IED	Intelligent electronic device
IT	Information technology
LAN	Local-area network
LPG	Liquefied petroleum gas
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
OT	Operation technology
PF	Pool fire
PLC	Programmable logic controller
ROI	Return on investment
ROSI	Return on security investment
RTU	Remote terminal unit/Remote telemetry unit
SCADA	Supervisory control and data acquisition
VCE	Vapor cloud explosion
VLAN	Virtual local-area network

This page intentionally left blank

1 Introduction

Globalization and the rise of Internet have pushed massive changes to the world we are living in today. Information and Communication Technology (ICT) is often regarded as one of the main drivers of the third industrial revolution as it penetrates deep into various sectors and changes the way people do things. For instance, it is evident how the information technology system has deeply integrated into our financial system, or how the communication system has become the foundation of many other systems.

Gradually, this transformation has resulted in what is called networks-of-networks, which is a term to illustrate how various kinds of systems are now interconnected. The interdependencies between systems have called for a shift in our thinking from component-oriented thinking towards network-oriented paradigm. In the past, engineers and experts would have easily scoped their goals and objectives within a single component. However, the connectivity between components has pushed forward the need to think how a component may influence another component in a connected system. The complex interconnected and interdependent systems have led to complications and risks that warrant new lines of research.

1.1 Problem Background

1.1.1 The Risk of Cascading Effects

Cascading effect is a consequence of the interconnectivity and interdependency of components in complex systems. Cascading effect is a phenomenon in which an initial event (e.g., component failure) in one part of a system propagates and spreads into its adjacent parts. In the case of cascading effect, the total consequence of the event is substantially larger than the sole impact of the initial event.

> **Cascading effects** – A phenomenon in which a primary incident propagates within a component, and/or to nearby components, either sequentially or concurrently, triggering one or more secondary incidents, resulting in overall consequences more severe than those from the primary incident alone[1].

Cascading effects have occurred in various kinds of complex systems and have been documented in several articles and literature. Some examples are cascading effect in an electric/power grid (U.S.-Canada Power System Outage Task Force, 2004), in a chemical and process plant (Lewis & Macalister, 2010), in information technology systems (Usborne, 1998), and also in non-engineering

[1] There are various definitions of cascading effects. This definition of cascading effects is adopted from G. Reniers and Cozzani (2013). A more comprehensive discussion of cascading effects definitions is presented in Subsection 3.1.1 (pg. 19).

systems such as financial system (Battiston et al., 2007) and ecological system (Sahasrabudhe & Motter, 2011).

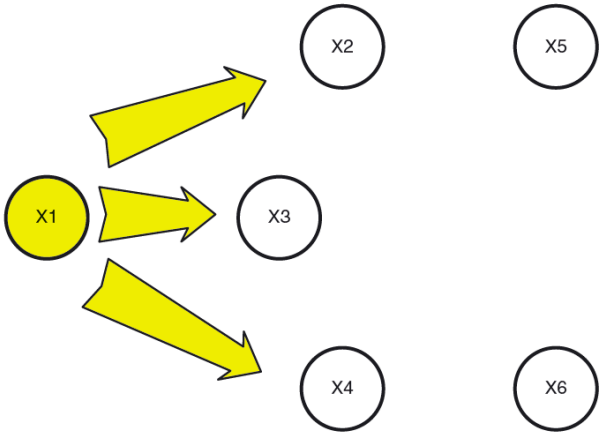


Figure 1. Illustration of cascading effect example: accident in X_1 potentially trigger other accidents in X_2, X_3, and X_4 (Khakzad et al., 2013)

Cascading effect can be triggered by various kind of incidents, although the type of triggers mainly depends on the type of the system. For example, a hazardous liquid leak in chemical plants, a component failure which causes transmission line overload in the power grid system, and a bankruptcy of a company in the financial system, all could potentially trigger cascading accident in their respective systems.

The main factor that enables cascading effects, however, can be quite similar across these different systems. Dependencies and interlinkages between units or components in a system are considered the main enablers of cascading effects (Khakzad & Reniers, 2015). For example, if component B is linked to and dependent on component A, then a failure in component A could cause component B to fail. In a sense, the failure spreads from component A to component B. Moreover, if there are more components directly or indirectly dependent on component A or B, then the failure might spread to those components as well. Such a situation where a failure spreads and causes a more widespread failure is called a cascading effect.

Even worse, in addition to interdependencies at the component level, interdependencies can also be observed at the system level. A situation where systems from different sectors are interlinked and highly interdependent have enabled cascading effects to propagate from one system to another, which potentially triggers cross-sectoral system failure.

1.1.2 Cascading Effects in Chemical and Process Plants

One particular type of system which prone to cascading effects is chemical and process plants. Chemical and process plants (or chemical plants) are a type of industrial facilities that process or produce chemicals. These types of facilities are typically large in scale and include the facilities for production, distribution, and storage of chemical substances. Examples of chemical plants include, among others, petrochemical plants, oil and gas refineries, and pharmaceuticals plants. The complexity of chemical plants, which mainly driven by interlinkages and dependencies between their components, have made it possible for an unwanted incident to cause widespread damage (Khakzad & Reniers, 2015).

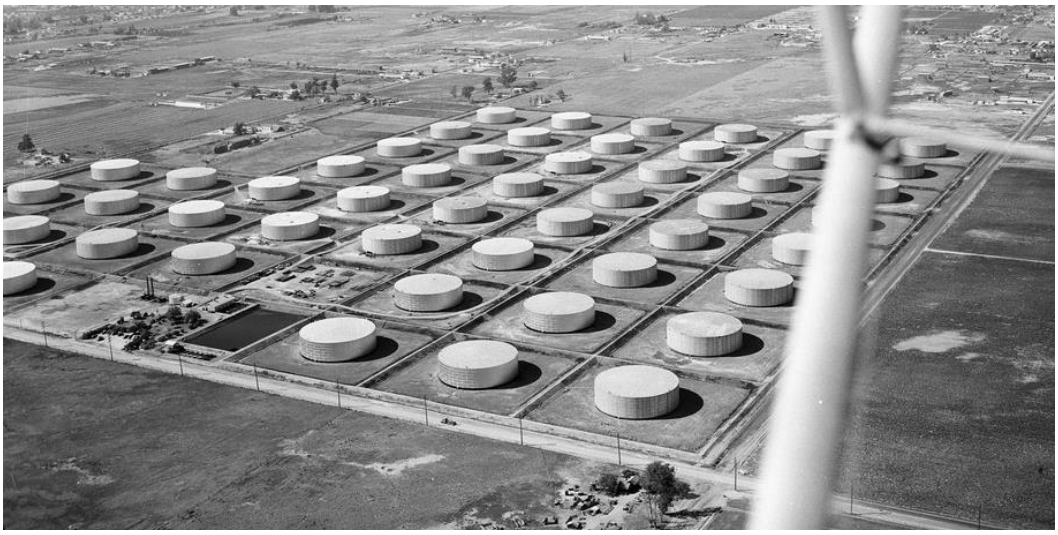


Figure 2. Aerial photo of chemical storage tanks (also called a tank farm).

Cascading effects on chemical plants have been witnessed to occur several times in the past. In 1984, a series of explosions happened in a large Liquid Petroleum Gas (LPG) distribution and storage center in San Juan Ixhuatepec, 20 km north of Mexico City. The accident, also known as the San Juanico disaster, started with an LPG leak which built up a vapor cloud allegedly due to a pipe rupture (Arturson, 1987), which was slowly blown to an ignition source by the wind. Around 5:00 am, the ignition of the vapor cloud resulted in an explosion, which led to a dozen more explosions within the next hour. As consequences, more than 500 people were killed, and the facility was destroyed. A more recent example happened in 2005 when Buncefield oil depot in England suffered a series of explosions from an overflow of fuel in one of its tanks. The incident was caused by the failure of two different safety devices to prevent the tanks from overflowing. The fuel leakage led to a buildup of a massive vapor cloud, which later got ignited by a spark, leading to fires and explosions. The series of fires and explosions propagated and spread to the adjacent tanks, resulting with more than 20 tanks caught in fires. The fire raged for almost two days, leading to 43 people being injured and the destruction of homes and businesses around the incident area (BBC, 2006; Khakzad & Reniers, 2015; Lewis & Macalister, 2010). These examples not only show the historical evidence of cascading effects in chemical plants, but also show that their occurrence would be followed by a catastrophic damage and loss.

On a side note, it is important to recognize and understand that chemical plants are classified as *critical infrastructures* by several governmental bodies (Ministerie van Veiligheid en Justitie, 2015; U.S. Department of Homeland Security, 2017). Critical infrastructure is a term used to represent facilities that are considered significant to society and economy. With regard to cascading effects, the classification is important for two reasons. First, being a critical infrastructure indicates that chemical plants might be interlinked to other kinds of critical infrastructures. This condition might allow cascading accidents to spread from one system to another (Barrett et al., 2010; Kotzanikolaou et al., 2011; Rinaldi et al., 2001). Second, being a critical infrastructure also suggests that chemical process plants at risk of attack from specific groups of actors due to their criticality and importance to the society. The latter indicates a possibility of cascading accident in chemical plants to be triggered by an attack.

1.1.3 From Cyberattacks to Cascading Accidents

Many critical infrastructures in general, and chemical plants in particular, have taken a path into digitization through the adoption of *Industrial Control Systems* (ICS) to manage and automate its industrial processes. The term ICS refers to several kinds of electronic equipment that are used to

control industrial processes, such as production and manufacturing. There are several types of ICS, namely Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Programmable Logic Control (PLC).

> **Industrial Control System (ICS)** – A group of hardware and software used to control and automate industrial processes, such as production and distribution. Nowadays ICS is already widely adopted and can already be found in critical infrastructures in various sectors, including chemical and process plants.

The wide adoption of ICS can be attributed to its business advantages including improvements in system performance, increasing reliability, and reduction in operating costs through automation. Today, ICS can be found in industrial facilities in various sectors and also in critical infrastructures.

Figure 3. A photo of SCADA system[2].

However, despite the number of advantages offered by ICS, their adoption by critical infrastructures has been subjected to scrutiny regarding its vulnerability against cyberattacks. In the past, most of industrial systems were not designed with security in mind. They were mostly proprietary and diverse systems (i.e., not mass produced) and were running in isolations. It is also said that these systems were relying on security by obscurity[3]. However, as industrial control systems developed, IT capabilities are increasingly integrated into ICS components, which have made ICS components more interconnected and less isolated (ICS-CERT & NCCIC, 2016). Moreover, as industrial control systems become more closely integrated into the less secure network (i.e., business network or corporate network) by the integration of SCADA system, they have become less isolated and more

[2] Steag. (2005). "Control room of a moving grate incinerator for municipal solid waste. The screen shows two oven lines, of which the upper ('Linie 1') is not in operation" [photograph]. Retrieved from https://commons.wikimedia.org/wiki/File:Leitstand_2.jpg#/media/File:Leitstand_2.jpg. The illustration is licensed under an Attribution-ShareAlike 3.0 Unported <https://creativecommons.org/licenses/by-sa/3.0/deed.en>.

[3] Security by obscurity (or security through obscurity) refers to the reliance on the secrecy of vulnerability as a security measure. This is not a recommended security measure as often there is no real security measure implemented, and the discovery of the vulnerability would result in a security breach (ICS-CERT & NCCIC, 2016).

exposed. Additionally, the adoption of commercial off-the-shelf (COTS)[4] components by ICS manufacturers may have increased the vulnerabilities of ICS components through, among others, a more rapid discovery of ICS security vulnerability in COTS products (Miller, 2006). In short, the increase of connectivity and the use of mainstream components in ICS have made these systems more vulnerable to cyberattacks. The adoptions of ICS by critical infrastructures have drawn concerns regarding the security of these facilities.

There have been several accidents involving cyberattacks towards ICS. Some examples of cyberattacks on ICS are the Stuxnet, a malware which was allegedly designed by the U.S. to attack Iran's nuclear program (Sanger, 2012), and a cyberattack on a German-based steel mill (Lee et al., 2014). In the steel mill accident, a hacker gained access to the network inside the facility and prevented a blast furnace from shutting down in a normal sequence, and as a result, the blast furnace was damaged. A more recent example happened in August 2017, where a petrochemical company in Saudi Arabia was attacked by a string of cyberattacks (McMillan, 2018; Perlroth & Krauss, 2018). The investigators suspect that the cyberattack was meant to sabotage the plant's operation and trigger an explosion by targeting the plant's safety controllers, which it failed to accomplish due to a bug in the attacker's computer code. However, it is presumed that following the failed attempt, the attackers would have already fixed the bug, and the same cyberattack can be pursued against nearly 18,000 plants that employ the same safety controller.

However, despite the reported vulnerabilities and the existing evidence of cyberattacks toward critical infrastructures, currently, there has been no record of cascading accident in critical infrastructures (or chemical plants) from a cyberattack. Nevertheless, there is also no strong reason why a cascading accident from a cyberattack cannot happen. Instead, there are a number of arguments to suspect the opposite.

First, despite without any recorded cascading accident, the recent successes of cyberattacks toward ICS in various critical infrastructures are still alarming. The past incidents have indicated that, with the right skill sets and a sufficient amount of resource, a cyberattack is capable of inflicting physical damage in critical infrastructures. Also, the instrument for cyberattacks is usually in the form of codes, which can be easily duplicated or modified. Therefore, a set of malicious code that has worked in the past is potentially also effective if used against other kinds of facilities, including critical infrastructures (Martellini, 2013). Moreover, the recent cyberattacks against critical infrastructures hinted that these actions were driven by different motives than economic motives. For instance, in the attack against the Saudi's petrochemical plant, it was believed that the attack was not meant to destroy data or to cause shut down to the plant, but to trigger an explosion that would have caused casualties. This evidence might imply that cyberattacks have gone from stealing information to destroying physical facilities.

Second, several studies have indicated that intentional attack is a likely cause of a cascading accident (Crucitti et al., 2004; Wang et al., 2014; Zhao et al., 2004). One of the main reasons is that most real-world networks that exist these days are highly heterogeneous systems, which have shown robustness against random failures but vulnerable to intentional attack. Moreover, several studies have specifically indicated how a cyberattack might lead to cascading accidents. Srivastava and Gupta (2010) described a hypothetical case in which a cyberattack potentially leads to a cascading effect. Boyes (2013) also suggests that if there is such a cybersecurity vulnerability which might result in a cascading accident, it is only a matter of time before an irresponsible actor triggers the accident. All in all, researchers have indicated that it is likely for intentional attacks (including cyberattacks) to cause cascading effects, especially in complex systems such as critical infrastructures.

[4] Commercial off-the-shelf (COTS) is a term to represent mass-produced items that are available for sale to the general public. A custom item that is specifically built based on a customer's requirement is not a COTS item. Microsoft Windows operating system and smartphones made by Apple are some examples of COTS items.

Third, it is widely understood that in adversarial risk assessment, vulnerabilities can be deemed as trivial unless there is an identified actor that might exploit them. According to De Bruijne et al. (2017), there are several classes of threat actors that have been identified to be threats to critical infrastructures, namely state actors, state-sponsored networks, and cyber-terrorists. In the Saudi's petrochemical plant case, it was believed that a nation-state actor was responsible for the cyberattacks. The primary indicator is that such an attack would require an enormous financial resource to carry out, yet there was no apparent monetary benefits can be gained from it (Perlroth & Krauss, 2018).

The mentioning of nation-state actors in cyberattack discussion and their motive can also be understood from the so-called cyber warfare. Cyber warfare can be defined as offensive actions taken by a nation, in the form of espionage or sabotage, to cause damages or disruptions to another nation through the cyberspace. For example, one Pentagon official stated how China had been developing possible alternatives to disrupt Taiwan's critical infrastructures (The Washington Times, 2004). Recently, FBI and Department of Homeland Security of the US also warned that North Korea might have developed a malicious software to attack critical infrastructures in the US and around the world (Gertz, 2017). In addition, it has been reported that several other countries have already begun developing their cyber capabilities (Kramer, 2016; Lim, 2017; Packham, 2017; Park & Pearson, 2017). The news has indicated that countries have been preparing for cyber warfare, and critical infrastructures such as chemical and process plants are among the potential targets.

Lastly, an explicit hint can be derived from governmental policies and allocation of resources in several countries to secure their critical infrastructures from cyberattacks. In 2013, the President of the United States signed an executive order to improve cybersecurity for their critical infrastructures, declaring that cyber threats to their critical infrastructure as "the most serious national security challenges" (Schmidt & Perlroth, 2013). This policy was reiterated four years later by a different administration when another executive order was signed to further improve the cybersecurity of their critical infrastructures (Volz, 2017). The Government of the United Kingdom also released a similar policy in 2016 (Asthana & Elgot, 2016). The policy set the UK Government to invest GBP 1.9 billion in reinforcing their cybersecurity, and the policy clearly emphasizes the need to protect critical national infrastructure in various sectors from cyberattacks. These actions seem to further reaffirm the concern about the possibility of cyberattacks on critical infrastructures.

In conclusion, the identified cyber vulnerabilities in critical infrastructures, the possibility of cyberattacks to result in cascading effects, and the existence of motivated actors that might exploit these vulnerabilities, strongly indicate that the risk of cascading effects from a cyberattack is real. Knowing the possibility of cascading effects in critical infrastructures (and chemical plants) and the severity of its consequences, the increasing vulnerability against cyberattacks in these facilities, which might lead to such accidents, must be mitigated. The risk of cyberattack-related cascading effects should call for further studies on this subject.

1.2 Problem Statement and Knowledge Gap

The previous sections have described how cascading effects potentially result in devastating consequences. Moreover, the recent successes of cyberattacks on ICS in industrial facilities implies that chemical plants and other critical infrastructures are also at risk of cyberattacks that targets ICS components. Although it has never happened before, a number of studies have pointed out how cascading accidents are likely to be triggered by intentional attack in general and cyberattacks in particular. Lastly, seeing the current state of policy developments by several countries to reinforce its cyber capabilities in protecting their critical infrastructures, it is concerned that an attack on critical infrastructure might happen at any time soon.

Problem Statement – There is a serious concern that the implementation of ICS across chemical and process plants might increase the risk of cascading effects across these facilities. Considering the vulnerability of ICS against cyberattacks, mitigation effort should be made to avoid disastrous consequences from cascading effects in the future.

Nevertheless, despite the possibility of cascading accident to be triggered by a cyberattack on chemical industries, such study has never been pursued. Hence, this research aims to contribute to the analysis and mitigation of cascading effects, particularly focusing on ICS vulnerability within chemical plants.

1.3 Risk-Based Network Segmentation for Cascading Effects Mitigation

Having recognized how ICSs might have increased the risk of cascading effects, mitigating the vulnerability of ICS components becomes the obvious way to mitigate the risk of cascading effects from this attack vector. Looking at the collaboration of private and public entities to reduce the risks of ICS incidents (e.g., through ICS-CERT[5] in the United States), it can be suggested that the effort to address vulnerabilities in ICS has already been widely pursued. However, it does not imply that the possibility of cascading effects in critical infrastructures from ICS-based cyberattacks can already be ignored. In fact, there are still several reasons to think that the risk of cascading effect from ICS-based cyberattacks should still be highly considered.

For instance, Bologna et al. (2013) found that most of the major attacks on critical infrastructures between 2010 and 2013 have utilized zero-day exploits[6]. How critical components in industrial facilities could suffer from such vulnerabilities can be understood by understanding the nature of ICS. Different from its IT counterpart, ICS components cannot be easily switched off because they are vital to the process and operation in industrial plants. These systems are expected to operate continuously for months, and, in some cases, even for years (Knapp & Langill, 2014). Switching ICS components off is almost always equal to stopping the plant's operation, which would be costly from the business perspective. Since applying security patches require the equipment to be switched off and restarted, this particular characteristic would make businesses and companies reluctant to apply security patches. Moreover, to avoid unwanted system conflicts, SCADA (a type of ICS system) servers are rarely patched (Fovino et al., 2009). Due to these reasons, patching ICS components can be deemed economically unjustifiable (Cardenas et al., 2009). Thus, it is possible that vulnerabilities could remain unpatched for an extended period despite the readiness of a security patch.

The poor patch management is just one of the reasons. Other factors such as careless equipment configuration, the tendency to cling to legacy systems, the lack of security training and weak policy enforcement, and ICS components that are discoverable through the Internet have potentially contributed to the increasing security vulnerability of the ICSs. Even if it can be assumed that an organization manages to perfectly implement every single best practice in cybersecurity to protect their assets, their security measures still would not be a match for targeted, sophisticated cyberattacks by nation-state actors (Bochman, 2018). All in all, it can be suggested that it would be

[5] Industrial Control System Cyber Emergency Response Team (ICS-CERT) is an organization that operates under the Department of Homeland Security of the United States of America. The mission of ICS-CERT is "to guide a cohesive effort between government and industry to improve the cyber security posture of control systems within the nation's critical infrastructure."

[6] A zero-day exploit (or zero-day vulnerability) refers to a publicly unknown vulnerability of a software or hardware that can be exploited by malicious actors. After the manufacturer has developed a patch for the vulnerability, the exploit is no longer called a zero-day exploit.

a very complicated task to prevent every possible cyberattack to ICS. At its worst, cyberattacks remain a possible precursor to cascading accidents.

However, regarding the risk of cascading effects, there is an alternative approach that can be taken. Referring to the *bowtie method*, risk management can be approached from two different perspectives: preventing the accident from happening (lowering the probability) or decreasing the impact of the accident (reducing the consequence). Considering that completely preventing ICS-based cyberattacks is difficult, then limiting the impact of cyberattacks to chemical plants can be a promising alternative to mitigate the risk of cascading effects. Pursuing this approach means accepting the fact that a certain amount of damage (from the cyberattack) would still occur. However, with regard to cascading effects, this approach may assure that no secondary accidents might follow the initial accident, thus cascading accidents can be avoided. So, the main premise is by managing the potential damage from cyberattacks, the cascading accident can be prevented.

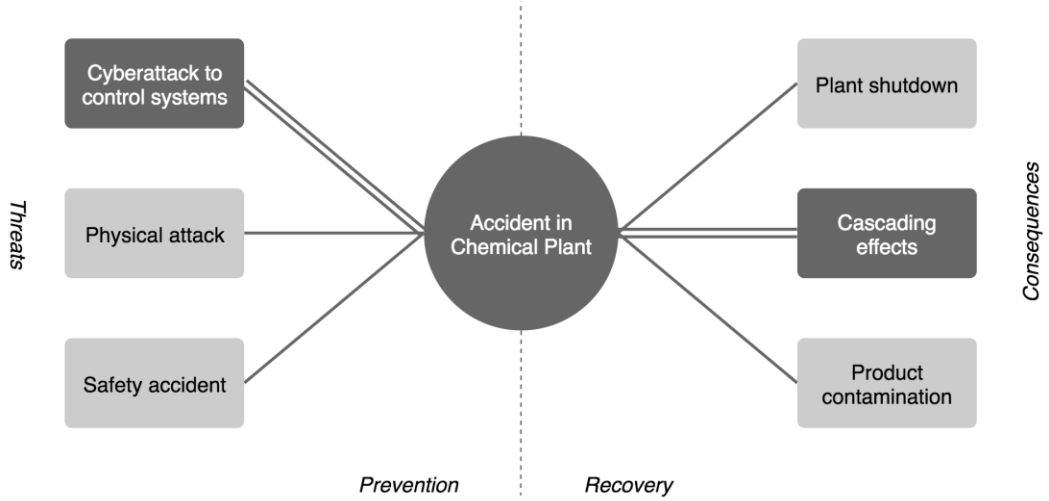


Figure 4. This bowtie diagram illustrates how the present work is related to cybersecurity and cascading effects analyses. The scope of the present study has been identified with double-lines and darker shade.

One of the control measures commonly used to limit the potential impact from cyberattacks is *network segmentation*. Network segmentation, sometimes also referred to as *network segregation* or *network enclave*, is the practice of partitioning the network architecture of ICS components into multiple smaller segments. As a common approach for improving cybersecurity, network segmentation works by creating several separate segments within a network, thus reducing the link between groups of components to the others. The remaining connection between the different segments can be protected using a firewall or other security hardening measure. By using this control measure, the impact of a security breach would be contained within a segment, and more widespread damage can be avoided.

> **ICS Network Segmentation** – A control measure of partitioning an ICS network architecture into multiple smaller segments.

Since network segmentation has been widely recognized to reduce the impact of cyberattacks, the next step is to find a way how network segmentation can be utilized to reduce the likelihood of cascading effects. One possible solution is to incorporate a *risk-based design* to the setup, design, or configuration of network segmentation of chemical plants. Adapting risk-based design definition from Vinnem (2014), the main idea of risk-based design is that some of the design decisions are

made based on the risks being considered, instead of, for example, following solutions from previous projects or adhering to existing standards.

> **Risk-based Design** – In the risk-based method, design decisions for protective and mitigative measures are taken according to the risk being considered instead of, for example, according to previous projects, regulatory requirements, or existing standards.

By understanding the risk of cascading effects and how cyberattacks might translate to accidents in chemical plants, segmentation in ICS networks can be designed in such ways that the resulting accident from a cyberattack imposes the least risk of cascading effect. The design of a network may determine the possible accident scenario and also the possible escalation targets. Some scenarios are worse, and some others are better regarding its likelihood to lead to cascading accidents. In that sense, by carefully designing the segmentation of the network, the risk of cyberattacks to lead toward cascading accident can be minimized. More specifically, through the application of the risk-based method, the probability of escalation of accident can be reduced, which in turn may reduce the likelihood of cascading accident.

Understanding the characteristics and the factors of cascading effects are crucial for developing a mitigation strategy for cascading effects. For instance, reducing the likelihood of an accident to propagate to nearby units (also known as the *probability of escalation*) can be the key to reducing the risk of cascading accidents. The probability of escalation depends on several factors, such as the intensity of *escalation vector*. Escalation vector refers to the amount of energy release from the initial incident to the affected unit(s). Examples of escalation vectors are heat radiation, overpressure, and fragment projection. The higher the intensity of the escalation vector, the higher the probability of escalation. By strategically designing a segmentation design, total escalation vector resulted from an attack can be reduced, and in turn, may also reduce the probability of escalation.

To conclude, the risk-based approach to ICS network segmentation in chemical plants potentially reduces the likelihood of cyberattacks to evolve to cascading effects. Therefore, a risk-based methodology for cascading effect mitigation from a cyberattack will be developed in this work. Although risk-based approach to ICS network segmentation would not be the silver bullet for cascading effects, a strategy to help reduce the risk of catastrophic events such as cascading accident is worth to be pursued.

This page intentionally left blank

2 Research Description

The background problem of this study has been introduced in the previous chapter. In the following section, the research objective is described. Firstly, the research objective is translated into the main research question and sub-research questions in Subsection 2.3. The relevance of this study toward scientific and practical domain is elaborated in Subsection 2.4. Lastly, the Subsection 2.5 describes how the structure of chapters and sections in this thesis explains the work undertaken in and the deliverables of this study.

2.1 Research Objective

This master's thesis presents an analysis regarding how the design of network segmentation in ICSs can be engineered to mitigate the impact of cyberattacks on cascading effect. More specifically, this research aims to analyze how the risk of cascading effects can be reduced through the application of risk-based approach to ICS network segmentation. Moreover, considering several factors such as the degree of complexity and access to sources of expertise, a case study of a chemical plant is used to help achieve the objective of this work. Hence, the following research objective is formulated:

> **Research Objective –** To develop a risk-based methodology for developing ICS network segmentation in chemical and process plants that will improve the systems' robustness against cascading effects from intentional attacks originated from the cyber domain.

Therefore, the deliverable of this thesis is a methodology for developing ICS network segmentation which employs a risk-based method for cascading effects mitigation. To develop the methodology, the present study employs a graph-theoretic approach developed by Khakzad and Reniers (2015). The graph-theoretic approach is adopted to help assess the criticality (or robustness) of network segmentation designs against the risk of cascading effects. Moreover, to enhance the validity of the methodology, this study also adopts a Bayesian network methodology developed by Khakzad et al. (2013). The Bayesian network methodology possesses several important foundations in analysis malicious attackers, such as being probabilistic in nature and ability to represent effects from multiple accidents (known as *synergistic effect* Khakzad et al. (2013)).

2.2 Scope and Assumptions

Following the research objective of this thesis, this section describes the scope and boundaries of this study. Incorporating several aspects from cascading effects, critical infrastructures, and industrial control systems might result in a very broad scope of the study. A careful and detailed determination of the research scope is necessary since not only each of these topics already constitutes a broad subject on their own, but also to ensure the focus of this work. In this section,

several aspects are briefly explained to describe the scope of this research. Also, the scope is presented in terms of an overview of what type of information is included in this study, while the boundaries (or limitations) are described as the circumstances that are not taken into account of this research.

Context

This study focuses on mitigating the risk of cyberattack-related cascading effects in chemical and process plants. In general, chemical plants are a suitable context for cascading effects research because of a few aspects. First, there is apparent interdependencies and interconnectedness in its components. Second, there has been evidence of cascading effects happening in chemical plants in the past. Lastly, many chemical plants in the world have adopted ICS into its system, making cyberattack-related cascading effects possible.

Cascading Effects Mitigation vs. ICS Vulnerability Mitigation

It needs to be reemphasized that this research aims to reduce the risk of cascading effects through the modification system layout, not to mitigate the vulnerabilities of ICS in itself. This boundary implies that the vulnerability of ICS components will be taken as is, and the direction of this research will not be aimed toward mitigating these vulnerabilities.

Threat Agent

In its application, a risk assessment methodology that includes attacker representation will involve a list of the potential attackers that are considered as threats to the business or organization that is being analyzed. The list of potential attackers, also called attacker profiles, usually consists of attacker archetypes along with their relevant characteristics.

The characteristics of the attacker profile to be used in this study are as follow:

- **Rational** – The threat actor is assumed to pursue a strategy that will yield the highest expected utility outcome for the attacker.
- **Unlimited cognitive and computational capability** – Realistically, the schematic of the target system could be complicated, making the formulation of rational strategy might not be feasible in a finite period of time. For simplicity purpose, it is assumed that the attacker will be able to formulate the best strategy possible regardless of the complexity level of the case study.
- **Perfect knowledge of the system** – The attacker is assumed to possess complete knowledge of the target system. Insider threat agent can also be assumed to possess complete system knowledge.

Static Environmental Factors

Several environmental factors such as humidity, air pressure, and the surrounding temperature may influence the result of the analysis. In reality, these factors are dynamic and may change randomly or regularly (e.g., daytime and nighttime). In this study, these environmental factors are going to be kept constant for simplification purpose.

2.3 Research Questions

In this section, the research questions are described. First, the main research question is logically derived from the research objective and the research scope. Afterwards, the main research question is further decomposed into several sub-research questions. The purpose of this section is to

breakdown the research objective into more specific and attainable goals, which then also serve as the guidance for the research processes. The main research question is as follow:

> **Main Research Question** – How to optimize ICS network segmentation design in chemical plants to improve its robustness against cascading effects under cyberattacks?

To help answering the main research question, several sub-research questions are developed. There are three separate domains relevant to this study: cascading effects, cybersecurity, and industrial control systems. A fundamental understanding regarding the three domains involved in this study is required, and these domains need to be reviewed especially in the context of chemical plants. Afterwards, the next step is to understand the background of the main problem of this research: the risk of cyberattack-related cascading effects in chemical plants.

> **Sub-research Question 1 (SQ1)** – How do cyberattack-related cascading effects happen in chemical and process plants?

Before the goal of robustness improvement can be achieved, a methodology to measure the level of cascading effect risk that sustained by network segmentation designs must be developed. For the present study, a Bayesian network methodology from Khakzad et al. (2013) is adopted as the methodology for cascading effect modeling and analysis. More specifically, this methodology allows several analyses such as probability measurement and propagation pattern modeling. Combined with the findings from SQ1, a methodology to estimate the risk of cascading effects for network segmentation designs based on BN method can be developed.

> **Sub-research Question 2 (SQ2)** – How to model and analyze cyberattack-related cascading effects using Bayesian network?

Once the method for cascading analysis has been developed, the next step is to develop a methodology to mitigate the risk of cyberattack-related cascading effects. The main purpose of the methodology is to facilitate the development of ICS network segmentations which show robustness against cyberattack-related cascading effects. To achieve the purpose, the crucial factors relating to network segmentation in ICS and cascading effects must be explored and discovered. Afterward, the findings on the crucial factors are used as inputs for developing the methodology.

> **Sub-research Question 3 (SQ3)** – What are the factors of ICS network segmentation design that can influence cascading effects in chemical plants? How can these factors contribute to mitigate cascading effects in case of cyberattack?

Lastly, the developed methodology must be evaluated to assess its effectiveness in increasing robustness against cascading effects. Moreover, this step is also useful to find opportunities for improvement for the methodology in the future.

> **Sub-research Question 4 (SQ4)** – To what extent does the segmentation design modification mitigate the risk of cyberattack-related cascading effects?

2.4 Thesis Outline

This thesis is divided into nine chapters organized as follow. Chapter 1 introduces the problem faced in this study, mainly explains the connection between cybersecurity and cascading effects in chemical plants. Following the problem introduction, the description of the research questions, the research objective, and the contributions of this study are presented in Chapter 2.

Next, Chapter 3 presents the findings from exploring some of the key domains of knowledge related to the topic of the present thesis, including cascading effects, industrial control systems (ICSs), cybersecurity related to ICSs and chemical plants, and network segmentation. Following the findings from the literature review, the approaches adopted for developing the risk-based methodology can be constructed and are described in Chapter 4. In Chapter 5, some of the aspects of network segmentation that relevant to cascading effects are explored. Afterward, based on the findings obtained in Chapter 5, the risk-based methodology can be developed.

Chapter 6 presents the development process of the methodology. The methodology development is described using a single case example throughout the chapter for the sake of clarity. In Chapter 7, the developed risk-based methodology is demonstrated using a case study, and the findings from the methodology development and demonstration are discussed in Chapter 8. Lastly, based on the process and the outcome of this thesis, several conclusions, including reflection of the work done and some future recommendations, are presented in Chapter 9.

3 Literature Review

This chapter discusses the existing peer-reviewed literature from various sources concerning the three main domains related to the present study: cascading effects, the industrial control system (ICS), and cybersecurity. The purpose of this chapter is to understand what has already been known about the three domains and also the state-of-the-art. Moreover, each of the three domains will be discussed in the context of chemical plants. It is expected that a solid understanding of the essentials of cascading effects, industrial control system, and cybersecurity can be achieved in this chapter. Also, more importantly, the understanding of these subjects is crucial to understand how cyberattacks possibly lead to cascading accidents, and to show that the solutions proposed in this study can be implemented to mitigate risks of cascading effects.

3.1 Cascading Effects in Chemical Plants

Cascading effect is one of the risks sustained by chemical facilities. The term cascading effect is used to represent phenomena in which an initial incident in one part of a system propagates and triggers another event to its adjacent parts. The initial events of cascading effects, or also known as triggering events, can be some random failures or intentional attacks. The resulting outcome of such phenomena could be a widespread system failure or even a collapse of an entire system. In facilities such as chemical plants, it can be imagined how a single explosion may trigger additional explosions due to the presence of flammable or combustible substances. Due to the severity of the potential impact, cascading effects are also considered as the most dangerous risk in chemical facilities (G. L. Reniers, 2010).

3.1.1 Introduction to Cascading Effects

G. L. Reniers (2010) classifies cascading effects into internal cascading effects and external cascading effects. The internal cascading effects constitute of cascading accidents that occur inside the boundaries of a single chemical plant. The external cascading effects represent cascading accidents that happen outside the boundaries of a chemical plant which the cascading effect initially starts. Due to the involvement of several chemical plants, these cascading effects are also called multi-plant cascading effects. Furthermore, Van Eeten et al. (2011) also mentioned how cascading effects might propagate into different sectors, potentially triggering a multi-sectoral collapse.

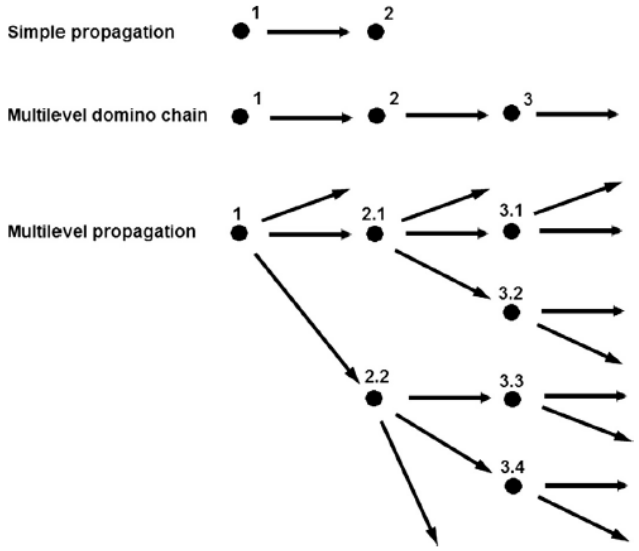


Figure 5. Examples of simple propagation, multiple-level domino chain and multilevel parallel propagation patterns (G. Reniers & Cozzani, 2013)

Moreover, cascading effect is also considered as challenging and difficult to manage due to several reasons. Firstly, cascading effects are typically regarded as low-probability and high-consequence event (Van Eeten et al., 2011). It means the accident frequency is very low and there is little statistical or historical data for researchers to use to analyze and study cascading effects, which makes the cascading effect difficult to mitigate. G. Reniers and Faes (2013) mentioned that due to its characteristics, managing and treating cascading effects requires a different approach than the typical occupational accidents. The second reason is cascading effect might involve different organizations across institutional boundaries. For instance, in the case of multi-plant cascading risk, the risk management effort requires much more multi-organizational agreement, collaboration, compared to managing internal cascading effect (G. Reniers & Faes, 2013).

3.1.1.1 Cascading Effects Definitions

There are various terms used to represent the phenomena in addition to "cascading effects." The term "domino effects," for example, has been commonly used in the existing works (Cozzani et al., 2005; Delvosalle, 1996; G. Reniers & Cozzani, 2013). Other terms that have been used, among others, "chain of accidents" (Khan & Abbasi, 1998) and "knock-on effects" (G. L. Reniers & Dullaert, 2008). These terms are frequently found in various literature and are used interchangeably to represent the same phenomena which have occurred in various domains.

Cascading effects have been described somewhat differently in by several authors, and the descriptions have also changed over time. Table 1 presents a non-exhaustive list of cascading effect definitions from various authors.

Table 1. Various definitions of cascading effects

Author(s)	Cascading effect definition
Delvosalle (1996)	A cascade of incidents in which the outcomes of an initial accident are increased by following one(s), as well spatially as temporally, resulting in a major accident.

Author(s)	Cascading effect definition
Khan and Abbasi (1998)	Situations which a fire/explosion/missile/toxic load resulting from an accident in a single unit in a plant causes secondary and higher-level accidents in other units.
Gledhill and Lines (1998)	Incident of loss of containment on a major hazard installation which resulted from a similar accident at an adjacent or nearby incident, either directly or indirectly. The events must have occurred at the same time or in close sequence, and the range of hazard from the domino incident must extend beyond the initiating event.
Cozzani et al. (2005)	An occurrence in which a primary incident propagates to nearby component, causing one or more secondary incidents, leading to overall consequences more severe than those of the primary incident alone.
G. Reniers and Cozzani (2013)	An accident in which a primary unwanted incident propagates within the same component (temporally), and/or to nearby components (spatially), either concurrently or sequentially, triggering single or more secondary unwanted incidents, which in turn potentially triggering further unwanted incidents, potentially resulting in more severe consequences than the those of the primary incident.

Cozzani et al. (2005) also described three main elements that characterize an event of cascading effects:

- A primary incident which triggers the cascading effect.
- A propagation effects caused by the primary incident, due to the effect of escalation vectors from the primary incident on secondary components.
- One or more secondary incidents, involving components from the same or different plant.

The primary incident is the initial event which triggers the propagating accidents, the secondary incidents are the incidents are initiated by the primary incident, and escalation vectors are the forces, or the physical effects, that cause the primary accident to propagate to nearby components (Khakzad et al., 2013). The characterizations from Cozzani et al. (2005) can be further complemented by a characterization offered by Khakzad and Reniers (2015), in which they stated to be regarded as a cascading accident, the total consequence of the chaining events must be substantially larger than the consequence of the primary event.

Cascading effects have also been witnessed to occur in various types of systems, such as communication system, power grid, and financial system. For the present study, it is not important to understand how cascading occurs in other domains. However, it is crucial to take into account that, albeit the similar failure propagation, the mechanism behind the phenomena in different kinds of domains can be very different. Therefore, the scope of the literature study must be carefully delineated to maintain the relevance of the present work. Several examples of cascading effects definitions from different domains are presented in Table 2.

Table 2. Definitions of cascading effects in different domains

Author(s)	Cascading effect definition	Domain
Kinney et al. (2005)	A breakdown of one component may not only have direct consequences on the performance of the network, but also may cause an overload which followed by partial or total breakdown of other components, resulting in a cascading effect.	Electric grid

Author(s)	Cascading effect definition	Domain
North American Electric Reliability Council (2005)	Rampant loss of system facilities, whether caused by thermal overload, voltage collapse, or loss of synchronism, except those that occurred due to fault isolation.	Electric grid
Battiston et al. (2007)	In a case of network economies, when a supplier (lender) fails to receive debt payment by its customer (borrower), who in turn may unable to pay its own supplier located in the upper level, which may lead to a chain of bankruptcies (bankruptcy avalanches).	Economics and Finance
Sahasrabudhe and Motter (2011)	The loss or serious suppression of a single or more species potentially propagate and cause other species to go extinct through the food-web network.	Ecology

3.1.1.2 History of Cascading Effects Accidents

Although cascading incident often regarded as a low-probability event, incidents involving cascading effect have occurred several times in the past. Abdolhamidzadeh et al. (2011) have developed an exhaustive list of incidents involving cascading effects, and the study presents a list of 224 incidents between 1917 and 2009 which known to involve cascading effects in the chemical process industry. Table 3 presents some examples of the recorded accidents.

Table 3. Examples of accidents involving cascading effects in process industry between 1917 and 2009. The list is taken from Abdolhamidzadeh et al. (2011).

Year	Location	Plant/unit (chemical)	Impacts
1917	Ashton, UK	Explosive factory (nitrator)	46 deaths, >120 injuries, 100 houses demolished
1947	Texas, USA	Ship (ammonium nitrate)	552 deaths, >3000 injuries, more than 3300 dwellings and 130 businesses damaged, and more
1974	Petal, USA	Salt dome storage (butane)	Glass breakage up to 11 km
1975	Beek, the Netherlands	Ethylene plant (propylene)	14 deaths, 107 injuries, damage in the radius of 4.5 km, 6 tanks burned, control room demolished
1979	Milligan, USA	Train of tank cars (ammonia, acetone, chlorine, and others)	14 injuries, 4500 people evacuated, $1.26 million damage
1984	Mexico City, Mexico	Storage tanks (LPG)	650 deaths, 6400 injuries, nearby houses damages, $31 million damage
1999	Laem Chabang, Thailand	Tank farm (gasoline)	7 deaths, 18 injuries, 4000 people evacuated
2001	Toulouse, France	Petrochemical plant (ammonium nitrate)	30 deaths, >5000 injuries, €2.4 billion damage
2005	Neyshabur, Iran	Rail tank car (variety of chemical)	328 deaths, 460 injuries

Year	Location	Plant/unit (chemical)	Impacts
2009	Jaipur, India	Petroleum products	500.000 evacuated, $40 million of property loss

From the cascading accident examples listed in Table 3, it is evident that cascading accidents have been witnessed in many parts of the world and the impact of such accident can be catastrophic. Moreover, cascading effects have occurred in different types of chemical facilities and involved different kinds of chemicals. More worryingly, Abdolhamidzadeh et al. (2011) also showed that global average of fatalities per accident is increasing. These findings indicate that cascading effects is a severe risk to various chemical plants worldwide, and therefore the risk of cascading effects should be accounted in the risk profile of these facilities.

3.1.2 How Cascading Effects in Chemical Plants Occurred

How the primary accidents are initiated is arguably one of the most important aspects of cascading failures. Initiating event, also called primary accident or triggering event, is the first component failure in a system that potentially triggers secondary failures in adjacent components. Initiating event is influential to the analysis of cascading effects because it largely influences the probability of cascading effect from happening. Understanding the triggers of cascading effects is important in the effort of mitigating the risk of cascading effects.

Clini et al. (2010) compiled a list of causes that have initiated the primary accident (i.e., the first accident) of cascading accidents. The list of causes, which compiled from data of accidents from 1950 until 2007, is presented in Table 4. From the table, external events and mechanical failures are two of the most frequent trigger of cascading accidents. Human factor as the third highest cause can be quite surprising since it suggests the need to improve the training or professionalism of the employees. It is worth noting that accidents caused by an attack (sabotage, terrorist attack, and military operation) are excluded from this list.

Table 4. General causes of cascading accidents. The list is adopted from Clini et al. (2010).

Number of events	Cause	Frequency
82	External events	31%
78	Mechanical failure	30%
54	Human factor	21%
46	Impact failure	18%
30	Violent reaction	11%
11	Instrument failure	4%
7	Upset process condition	3%
3	Service failure	1%

In addition to categorizing primary accident according to their causes, categorizing the primary accidents by the types of the accidents can be a useful alternative. The type of a primary accident is one of the factors that determine the escalation vectors in a cascading accident (Khakzad et al., 2013). The analysis on the types of accidents may provide insights on the escalation vectors, which

may help with the prevention of accident propagation since different escalation vector requires different mitigation method.

There are various types of accidents that can initiate cascading accidents. Khan and Abbasi (1998) and Clini et al. (2010) offered similar classifications of types of primary/initiating accidents. Clini et al. (2010) found that fire and explosion are the most frequent types of primary initiating accidents accounting for 43% and 41% respectively. The classifications of types of primary events in cascading accidents are presented in Table 5.

Table 5. Types of accidents that can initiate cascading accidents

Source	Classification

Khan and Abbasi (1998)	• Fire
	• Explosion
	  ○ Blast waves
	  ○ Missiles
	• Toxic release
	• Simultaneous and interactive impact of fire and explosion

Clini et al. (2010)	• Fire
	• Explosion
	• Release
	  ○ Liquid
	  ○ Gas
	• Gas cloud

Another perspective of triggering event analysis has been taken by researchers by categorizing the cause of initiating events into two categories: random failures or intentional attacks (Crucitti et al., 2004; Kinney et al., 2005; Wang et al., 2008). From the two categories, intentional attacks are understood to be the more probable cause of cascading effect in real-world networked systems. To further understand the difference between intentional attack and random failures in triggering cascading effect, some theory about complex networks have to be explored.

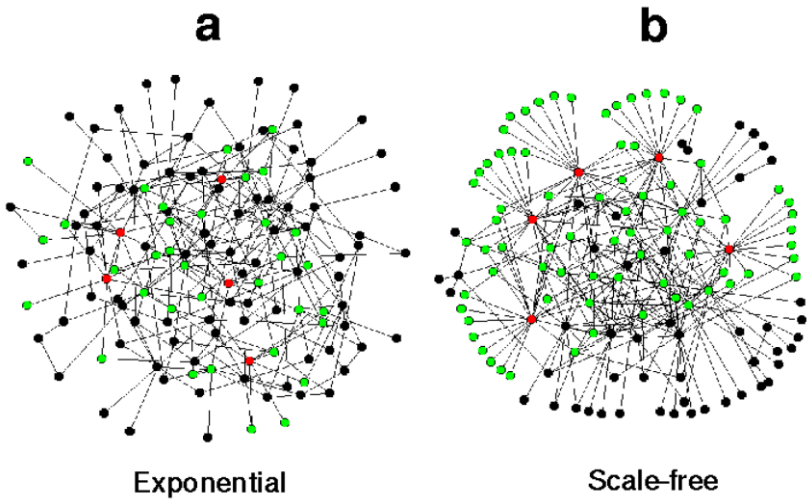


Figure 6. Illustration of (a) an exponential network and (b) a scale-free network (Albert et al., 2000)

Complex networks studies recognize two types of networks based on their connectivity distribution: *exponential network* and *scale-free network* (Albert et al., 2000). An exponential network is relatively homogeneous, meaning the nodes in the network tend to have similar number of links. On the other hand, a scale-free network is very heterogeneous; most of the nodes have one or two links, while a few nodes have a large number of links. The structure of scale-free network represents most of the real-world networks, such as the Internet and electrical power grid.

Several studies have shown that real-world networks are demonstrating robustness against random failure (Wang et al., 2014). This implies that the probability of cascading effect to occur because of a random event in nodes is small. However, the scale-free networks (i.e., most of real-world networks) have been indicated to be vulnerable against intentional attacks (Albert et al., 2000). For instance, it has been shown in the case of scale-free networks, an attack on a single node could lead to the failure of an entire network (Motter & Lai, 2002; Zhao et al., 2004).

These findings conclude that, compared to random failures, intentional attacks are the more critical precursor to cascading effects in real-world networks. Why the real-world networks are vulnerable against intentional attacks can be understood by examining the two fundamental characteristic differences between intentional attacks from random errors.

The first characteristic is related to the heterogeneity nature of scale-free networks; a few number critical nodes (i.e., with a significant amount of links) among the larger number of less significant nodes (i.e., with one or two links). In case of random failures, the failure events can be assumed to have the same probability of occurrence in any nodes in the system. Since the number of highly critical nodes are much smaller than the less significant nodes, random failures will likely to happen on the latter. However, the assumption is not applicable to intentional attacks because intelligent attackers can be assumed to target the most critical components in the system (Koç et al., 2013). This characteristic of targeting the highly critical nodes contributes to the susceptibility of networks with scale-free structure (i.e., most real-world networks) to cascading effects from intentional attacks.

The second characteristic is related to the fact that cascading effect is much more likely to happen when triggered by failures in two or more nodes. Multiple accidents are more likely to trigger cascading effects due to the interaction of escalation vectors (e.g., heat and projectiles) from the two or more accidents, resulting in a stronger escalation vector. The stronger the escalation vectors, the higher the likelihood of accident propagation. For example, in case of explosions in a chemical plant, the combined heat radiation from two explosions is more intense than that from a single explosion. This phenomenon is called the synergistic effect (Khakzad et al., 2013). With that being said, in the case of a random failure event, it is very unlikely to witness two nodes or more fail in the same moment because the risk of component failures is independent of each other. We argue that in case of intentional attacks, malicious actors will try to increase its likelihood of success by attacking more than a single component. Therefore, the probability of having two or more nodes to fail at the same time is much higher, thus increasing the risk of cascading effect.

3.1.3 Cascading Effects Involving Cyberspace

The risk of cascading effect is also present in the cyberspace domain. The Internet and the World Wide Web is composed of a vast number of interconnected dynamic components, which are some of the properties of complex networks (Boccaletti et al., 2006). Boccaletti et al. (2006) further stated that the dynamics of flows in a complex network might give rise to cascading effects. Van Eeten et al. (2011) also mentioned how accidents in interdependent critical infrastructures (CIs) in several sectors (including the Internet) potentially trigger cascading effects.

Although there has been no record of cascading effects in chemical facilities caused by cyberattacks, there has been some evidence on the occurrence of cascading effects on cyberspace domain or those that are triggered by an event from cyberspace.

The Galaxy IV satellite case is one of the examples of cascading failures from originating cyberspace. On 19th May 1998, around 90% of pager users in the United States experienced loss of service due to a short-circuit in the main control of the satellite. The loss of service also caused problems to the healthcare sector since hospitals were dependent on the service to contact doctors and emergency workers (Usborne, 1998). Moreover, the satellite failure also impacted other services such as television networks and credit card payment system.

A more recent example happened in 2017 when a malware known as WannaCry affected vulnerable computers around the world. WannaCry is ransomware which specifically designed to attack the older version of Windows operating system. The ransomware operates by encrypting the victims' files and then demands a sum of payment be made in exchange for the key to decrypt the files. One of the victims of this attack was England's National Health Service (NHS). The attack disrupted the NHS's services, resulting in activities such as x-rays and scheduled operations being stopped and postponed (Johnston et al., 2017). The Galaxy IV and the WannaCry malware incidents put into perspective how cyberspace and IT systems are vulnerable to cascading effects.

Furthermore, the cyberspace domain is potentially a more significant origin of cascading effects than commonly thought. Research based on public media has found that the Telecommunication and the Internet sectors together are the origin of 44% of cascading effects in the Netherlands, only second to the energy sector which accounts for 47% of all cascades (Van Eeten et al., 2011, p. 388). The important take away is that the deep integration of IT into various sectors has made it possible for an error from the cyberspace to propagate to and negatively impact the other domains. Depending on the type of the sector on the receiving end, the impact could be either negligible or catastrophic.

3.2 Cascading Effects Modelling and Analysis

Cascading effects are often regarded as low-probability and high-consequence events. Being a low-probability event implicates that there are extremely little historical data available relating to these incidents. This characteristic is the opposite of occupational accidents, which is the type of accidents with a lot of historical data. In the case of occupational accidents, the risks are typically managed using statistical and mathematical models based on past incidents. On the other hand, having a different characteristic indicates the risk of cascading accidents cannot be approached in the same manner as the occupational accidents. Instead, managing risks of cascading effects can be based on the scarcely available data, data generated through extrapolation, assumptions, and expert opinion (G. Reniers & Faes, 2013). Moreover, the process of determining its risks should utilize highly specific mathematical models and software.

On that ground, this study employs a cascading effects methodology by Khakzad et al. (2013). Khakzad et al. (2013) developed a Bayesian network methodology to estimate the path probability of cascading effect in processing facilities. The Bayesian network methodology is presented in the next section.

3.2.1 The Bayesian Network Methodology

Interconnectivity and (inter)dependency between components are the main enabler of cascading effects (Khakzad & Reniers, 2015). Therefore, in order to manage the risk of cascading effects, a methodology that is capable of modeling the complexity and interdependency of the system is required. Cascading effect characteristics are also the main reason why some linear models are

incapable of modeling such risk. Linear models such as Attack Tree and Fault Tree assume that events are independent of each other, which is not the case for an interdependent system.

One of the few models that are capable of handling interdependencies is the Bayesian network (BN). Causal BNs model is one of the modeling technique that has gained popularity over the last couple of years. BNs also has been recognized as one of the ideal techniques for risk assessment. BNs model can be described as a graphical notation of dependencies between variables. BNs model consists of nodes and edges which represent variables and causal relationships respectively. The strength of the links is represented in the form of a probability table. One of BN advantages that give rise to BN's popularity is its ability to update its prior belief in the light of new evidence. Other advantages of BN are the ability of BN to combine different sources of knowledge to overcome the challenge of scarcity of data, the ability to model a somewhat complex structure, and capacity to present multi-state variable. Some have argued that these characteristics give Bayesian Networks its advantages over the alternative models such as Fault Tree, Markov Chains, and Petri Nets (Weber et al., 2012).

Khakzad et al. (2013) develop a Bayesian network methodology to analyze cascading effect in a network. There are several advantages of this methodologies as compared to the existing methodologies. The nature of cascading effects is that it propagates through several levels in the network, starting from the initial failure. This methodology is capable of considering not only the first-level of the accident but also takes account the higher-level accidents. Different levels of incidents are referred to as primary event, secondary event, tertiary event, and so on. Moreover, the capability to account synergistic effects of different events in different levels has also enabled a more accurate estimation of the higher-level accident. Moreover, as a Bayesian network-based methodology, this method able to include both quantitative and qualitative inputs. The qualitative input is shown in the structure of the graphical models. As the components depicted as nodes and connection between them illustrated as edges, the configuration of nodes and edges in the graph represent the dependency between the components. The quantitative input is exhibited in the formation of conditional probability table (CPT). Additionally, as the nature of the Bayesian networks, the methodology is a probabilistic model. Also, being a Bayesian network-based method means this methodology support probability updating in the light of new information.

There are several important aspects to cascading effects that are represented in this methodology. First, the *accident propagation*. Accident propagation in this methodology is the investigation of how the primary event in an incident could escalate to the secondary event, how the secondary event escalates to the tertiary event, and so on. The accident propagation analysis is influenced by two factors, the *escalation vectors*, and the *threshold value*. Escalation vector can be defined as the measurement of physical effects such as heat radiation, overpressure, or projectile fragment that comes from an event of failure and may affect the nearby components. The threshold value is the amount of "damage" that can be sustained by a component before the component fails. Thus, by comparing the magnitude of escalation vector from the initial incident, and the threshold value of the nearby components, preliminary assessment of the vulnerable units can be done. Moreover, in a phenomenon is called synergistic effect, escalation vectors from two or more damaged components may interact and result in an even stronger escalation vector. Synergistic effects must be taken into account by considering escalation vectors of damaged components from different accident levels (e.g., failures from primary event and secondary event toward potential tertiary components). Considering the synergistic effects of events in different order allows more accurate analysis of events in the higher order.

The second important aspect is the *escalation probability*. Escalation probability is the likelihood of failure of certain components given an exposure of escalation vector from another damaged component. In such case in which an escalation vector surpasses the threshold value, it cannot be immediately defined that the component is damaged. Having an escalation vector exceeding a threshold value means the probability of damage in such situation cannot be neglected. Escalation probability is the likelihood of these components to be damaged. If the escalation vector is well

below the threshold value of a component, then it can be said that the escalation probability of the component is negligible. The calculation of escalation probability is done using the widely used probit[7] value (Khakzad et al., 2013). Probit value can be calculated using the equation below:

$$Y = a + b\,ln(V) \quad \text{Eq. 1}$$

Y being the probit value, *a* and *b* are the probit coefficients derived from experimental data, and *V* is the escalation vector. Once the probit value is obtained, the escalation probability can be calculated using the following equation:

$$P_{Escalation} = \phi(Y - 5) \quad \text{Eq. 2}$$

By taking into account these elements of cascading effects into the methodology, there are two analyses that can be done by using this methodology: determining the propagation path of cascading effects and calculating cascading (domino) probability. Once the propagation path of an accident is analyzed, the probability of cascading effects can be determined afterward. The following section presents the description of the Bayesian network methodology and how it works.

3.2.2 Graph Theoretic Approach for Identifying Critical Units

As will be explained in the next section, the analysis of cascading effects starts with identifying the most critical component in the system. As proposed by Khakzad and Reniers (2015), the most critical components in the system can be identified using graph theory metrics. Using the most critical component as the primary event in cascading effect analysis would lead to the most severe cascading accident scenario.

Some graph theory basics are essential for this analysis. A mathematical graph is comprised of *vertices* (plural for *vertex*) and *edges*. A vertex can be depicted as a node, while edge can be represented by a line. Moreover, there are two categories of metrics for graph metrics: vertex-level metrics and graph-level metrics. As the notions suggest, the vertex-level metrics are used to measure the criticality of vertices, and the graph-level metrics are utilized to compare different graph structures. These metrics are often referred to as *centrality*, which is a concept that encompasses different kinds of graph metrics. Three vertex-level metrics that are popularly used: degree, betweenness, and closeness. The degree centrality can easily be determined by counting the number of edges a vertex has. The betweenness centrality is quantified as the number of shortest paths between all combinations of vertices that transverse the vertex in focus divided by the number of shortest paths between all combinations of vertices. Lastly, the closeness centrality counts the number of steps required to reach all the other vertices in the graph.

Khakzad and Reniers (2015) stated that closeness centrality score indicates the criticality of a vertex in initiating cascading effects. The components with the highest closeness centrality score have resulted in the highest cascading probability. Hence, it is advised that preventive measures are applied to components with high centrality score to reduce the probability of cascading effects. Moreover, Khakzad and Reniers (2015) have also found that betweenness centrality score may contribute to mitigating cascading accident. It has been shown that "isolating" vertices with the largest betweenness scores have significantly limited the accident propagation in case of cascading effects.

[7] Probit (probability unit) can be defined as a unit of probability which is deviated from the mean of standard distribution. A probit method is a method that use probit value as their input.

Here: add from (Vulnerability analysis of process plants subject to domino effects) – here the efficacy of graph theoretic approach is thoroughly tested

3.2.3 Processes in Cascading Effects Modelling

3.2.3.1 Propagation Path Analysis

The first analysis that can be produced by using this methodology is to determine the likely propagation path. The propagation path is required for calculating the probability of cascading effects in a system. Overall, there are six main steps to develop the propagation path in a particular system. Below is the overview of steps in defining the propagation path by using the Bayesian network methodology:

- Assign a node to every component.
- Determine the primary component, which can be done by investigating the most critical components in the system. The method to determine the most critical component is explained in Subsection 3.2.2.
- Specify escalation vectors from the initial accident to the nearby component(s) (i.e., potential secondary component). The escalation vectors to the adjacent components depend on several factors (e.g., the type of accident, the distance between the components, etc.) and can be calculated using various methods.
- To determine the secondary components, the following steps are performed:
    a. For each potential secondary component, compare the escalation vector sustained in the component with the predefined threshold value. If the escalation vector sustained exceed the threshold value, then continue to the next step. Else, the escalation vector is assumed not intense enough to cause damage to the component.
    b. Calculate the probit value of each component. Probit value is a function of escalation vector.
    c. Using the calculated probit value, calculate the escalation probability of the secondary component.
    d. Once the escalation probabilities for all potential secondary components have been calculated, choose the component(s) with the highest escalation probability as the secondary component.
- After the secondary component(s) are determined, the type of accident and the probability of the accident are specified.
- If the system configuration enables higher-level cascading effects, repeat steps three to five by substituting the newly elected secondary component(s) for the primary unit. Also, when evaluating cascading effects on a higher level, the possibility of synergistic effects must be taken into account.

3.2.3.2 Calculating Cascading Probability

After the cascading propagation path of a system has been determined, then the probabilities of cascading in different levels have been calculated. To better understand how the cascading probability is calculated, take a hypothetical case in Figure 7 as an example.

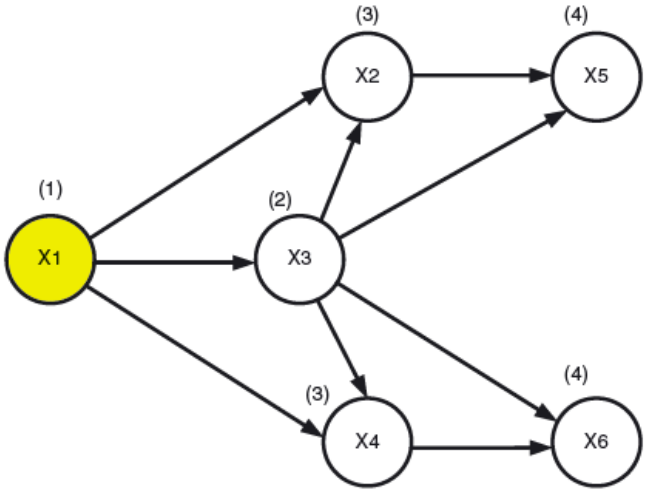


Figure 7. Accident propagation pattern of cascading effects (Khakzad et al., 2013)

Assume that a propagation pattern analysis has been done on a hypothetical system and the result is presented in Figure 7. In other words, Figure 7 illustrates the likely propagation path of the cascading effect in the example case. As shown in Figure 7, it has been estimated that the primary event would occur in component X_1, the secondary event occurs in X_3, the tertiary events occur in X_2 and X_4, and the quaternary events occur in X_5 and X_6. Moreover, the primary component is used for the components involved in the primary event. Similarly, the term secondary component(s) used for components in the secondary event, tertiary components for those in the tertiary event, and so on.

Now that the propagation path has been determined, the first step is to calculate cascading effects probability is to calculate the probability of cascading in the first-level. The probability of cascading effects can be calculated by multiplying the probability of the primary event and the escalation probability of the affected components. The formula to calculate cascading probability at any given level is:

$$P_{Cascading} = P(X_x) \cdot P(X_y|X_x) \quad \text{Eq. 3}$$

X_x being the primary component and X_y being the potential secondary component. In the case illustrated in Figure 7, the cascading effect is said to reach the first-level when X_3 has been impacted by failure from X_1. Using the formula in Eq. 3, the probability calculation for the first-level cascading effect can be calculated as follows:

$$P_{First\ level} = P(X_1) \cdot P(X_3|X_1) \quad \text{Eq. 4}$$

The next step is to calculate $P_{Second\ level}$. Looking at Figure 7, it can be observed that both X_2 and X_4 are potential tertiary components. Cascading effect is said to reach the second-level when either X_2 "or" X_4 is impacted by the first-level cascading effect.

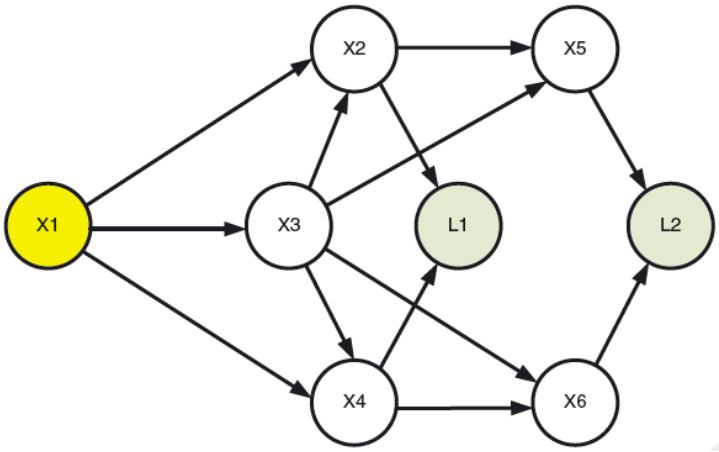


Figure 8. Accident propagation pattern with added auxiliary nodes (Khakzad et al., 2013)

To represent the second-level cascading effect, an auxiliary node L_1 can be added into the graph (see Figure 8). The node L_1 is equal to either X_2 "or" X_4 is affected by the events from $P_{\text{First } level}$ (see Eq. 5). Hence, the node L_1 equals to the union of X_2 and X_4, which is the failure probability X_2 or X_4. However, L_1 is not equivalent to the probability of cascading effect at second-level, but merely an auxiliary tool to calculate the likelihood of cascading effect at second-level. The probability of cascading effect in the second level can be calculated as follows:

$$L_1 = X_2 \cup X_4 \quad \text{Eq. 5}$$

$$P_{Second\ level} = P(X_1) \cdot P(X_3|X_1) \cdot P(X_2 \cup X_4|X_1, X_3) \quad \text{Eq. 6}$$

Similarly, the third-level cascading effect can also be represented by an auxiliary node. Auxiliary node L_2 means that either X_5 "or" X_6 is involved in the propagating accident. Again, L_2 is not the probability of cascading effect at its level, it merely an auxiliary node used to help with the calculation.

$$L_2 = X_5 \cup X_6 \quad \text{Eq. 7}$$

$$P_{Third\ level} = P(X_1) \cdot P(X_3|X_1) \cdot P(X_2 \cup X_4|X_1, X_3) \cdot P(X_5 \cup X_6|X_2, X_3, X_4) \quad \text{Eq. 8}$$

To further aid the calculation of cascading effects probabilities, another type of node can be added to the graph. In Figure 9, auxiliary nodes DL_1, DL_2, and DL_3 are added to the graph. Each of these nodes is representing the sequential level of cascading effect. Each of the nodes is connected to the other nodes as depicted in Figure 9 by AND-gate. For instance, the DL_1 node is connected to X_1 and X_3 by AND-gate. Hence $P(DL_1)$ equals to the probability of cascading effect in first-level. In case of DL_2, the node is connected to both DL_1 and L_1 through AND-gate, which means the first-level cascading effects must have happened, and the first-level accident must have propagated to the next level either toward X_2, X_4, or both. Therefore, $P(DL_2)$ equal to the probability of the second-level cascading effect. Accordingly, the same idea also applies to DL_3.

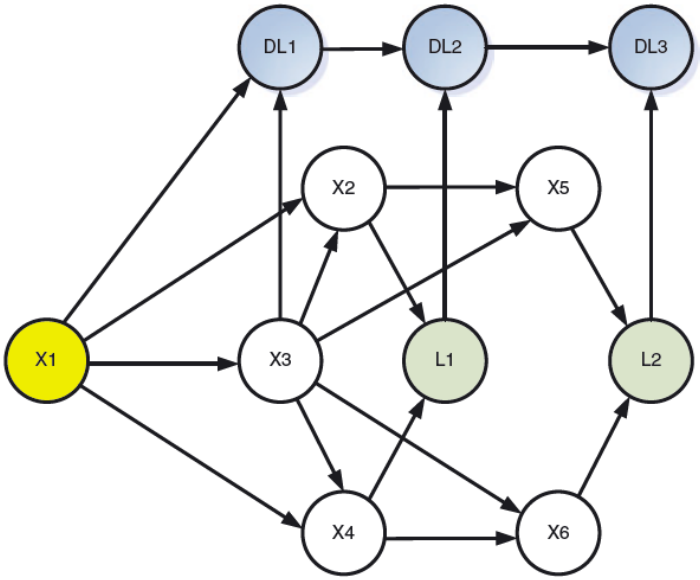


Figure 9. The complete accident propagation pattern graph (Khakzad et al., 2013)

3.3 Industrial Control Systems (ICSs) in Chemical Plants

In a discussion about cybersecurity of chemical plants, or any industrial plants for that matter, the topic of Industrial Control System (ICS) is indispensable to the discussion. ICS refers to a wide range of systems and components used to control operations in industrial facilities and critical infrastructures. Although ICS have actually existed for hundreds of years (Hayden et al., 2014), the issue with cybersecurity on ICS was started in the late 1960s when these control systems started to be connected to digital computers. Several trends such as the integration of control systems to the Internet, the use of commercial off-the-shelf (COTS) components, the integration of industrial network to the less secure business network, all of which have contributed to the increasing vulnerability of ICS against cyberattacks. These computerized control systems have become a new attack vector for different kinds of cyber attackers with various intents. To prevent cyber threats from exploiting ICS, it is important to understand how ICS actually works in real life. In the next section, ICS and some of the most frequently related terms in the ICS discussion will be described.

3.3.1 Definitions of ICS

ICS exists within a larger group of technology called the operation technology (OT). The use of operational technology has gained popularity over the last decades due to its ability to offer automation over industrial processes. The automation capability results in several benefits such as the increase in efficiency, an increase in reliability and a decrease in production cost.

Operation technology (OT) – An umbrella term that encompasses a group of technologies that support industrial operations. The term is more inclusive than ICS and often used to distinguish them from the traditional information technology (IT) system.

ICS itself is an umbrella term that encompasses a wide range of technologies and systems[8]. The implementations of ICS can vary considerably, from a relatively simple system such as a temperature control system to a massive and complex system such as in a region-wide power grid. Although the term represents rather broad and inclusive, the term has been quite consistently described by several authors. Several definitions of ICS are presented in Table 6.

Table 6. Industrial Control System (ICS) definitions.

Source	Definition
Stouffer et al. (2011)	"is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures."
Knapp and Langill (2014)	"is a broad class of automation systems used to provide control and monitoring functionality in manufacturing and industrial facilities."
Trend Micro (2016)	"is a collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes."

Many often confuse the term ICS with many other closely related terms, such as Distributed Control System (DCS), Supervisory Control and Data Acquisition (SCADA), and Programmable Logic Controllers (PLC). Essentially, these terms are used to represent different types of systems, or different system configurations, which are still within the ICS category. However, during their evolution, the functionalities of these technologies have expanded and eventually overlapped each other. Their overlapping functionalities may have led to the confusion as mentioned earlier.

Table 7. Definitions of DCS and SCADA (Stouffer et al., 2011)

System	Definition
SCADA (*Supervisory Control and Data Acquisition*)	SCADA systems are used to control, manage, and monitor assets dispersed over a large geographic area using centralized data acquisition and supervisory control.
DCS (*Distributed Control System*)	DCSs are used to control and automate industrial processes within a local area such as a factory.
PLC (*Programmable Logic Control*)	PLCs are locally installed equipment commonly used for controlling and regulating local process.

[8] US Department of Homeland Security (2004) classifies the following systems as part of the broader ICS term: Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Process Control System (PCS), Energy Management System (EMS), Automation System (AS), Safety Instrumented System (SIS), and any other automated system.

3.3.2 Components and Architecture Overview

Precisely defining what ICS comprises of can be rather overwhelming. On the one hand, it is because ICS can be composed of numerous types of components, and on the other hand it is because the sheer number of components are working on different layers in a hierarchical structure. Therefore, it is important to learn the different levels of ICSs to understand further what ICS is and how ICS works. The different levels of ICS can be depicted by the ICS architecture. In the following section, ICS components and subsystems will be described according to their respective layers in the ICS architecture.

There are several existing ICS reference architectures, such as the CPwE Architectures from Cisco, Purdue Enterprise Reference Architecture (PERA), ICS architecture by ICS-CERT and NCCIC, and many others. To describe ICS and the components it comprises of, this study is adapted the ICS architecture from ICS-CERT and NCCIC (2016). It is important to note that the objective of selecting one of the reference architectures is to have a realistic architecture that can be used as a reference for the present study. Therefore it is not imperative to have all the available options considered and evaluated. Moreover, despite their variations, these ICS architectures tend to be relatively comparable, and their terminologies are also interchangeable (Hadžiosmanović, 2014).

The ICS architecture from ICS-CERT and NCCIC (2016) comprises of seven different levels that contain different kinds of ICS components. Figure 10 illustrates a reference architecture for ICS. The bottom level contains Field Devices, continued with Controller LAN, Local HMI LAN, Manufacturing Zone, Demilitarized-zone (DMZ), Enterprise Zone, and Internet Demilitarized-zone (Internet DMZ). Each level may contain different kinds of components and serve different purposes. One important thing to note is the demarcation between Level 3 and Level 4 as depicted in Figure 11. Level 3 and the levels below (i.e., Level 0, Level 1, etc.) are often referred to as Operation Technology (OT), while Level 4 and the levels above (i.e., Level 4 and Level 5) are referred as Information Technology (IT). This segmentation also depicts the demarcation between the industrial network and the business network (also called corporate network or enterprise network), which is an important aspect when discussing the security of ICS network in Section 3.4.

In the next section, each level of the ICS architecture along with the component contained therein will be described.

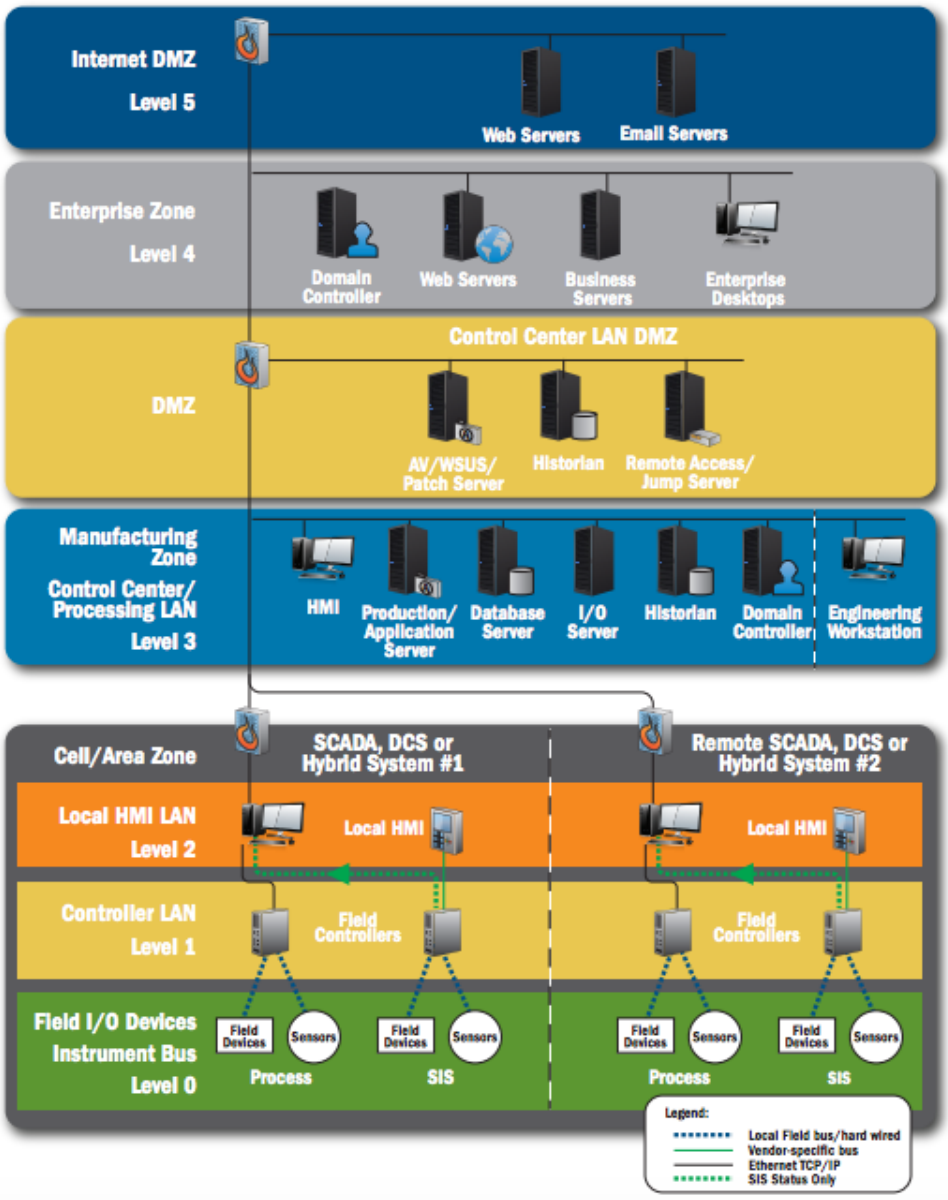


Figure 10. ICS Network Architecture (ICS-CERT & NCCIC, 2016)

3.3.2.1 Level 0: Field I/O Devices (Sensors and Actuators)

The first layer of the ICS architecture contains the basic elements for the rest of the ICS architecture. Primarily, this layer would be composed of three main components: sensors, controllers, and actuators. The first element is the sensors. The role of sensors is to gather information for the current state of the process. The information collected can be various, but mostly they are a physical property of the process. For example, in a water heating process, the temperature of the water is gathered using a thermometer. The information from sensors will be forwarded to a controller to be processed. Controllers are located on Level 1, and it will be described in the next section. The result of the process from the controller is forwarded back to an actuator. Actuators, sometimes also called the final control element, are components that translate commands into physical actions. Several examples of actuators are fans, pumps, valves, heater, and motors. It is also important to mention the object that is “sensed” by the sensor and “treated” by the actuator is an industrial process. The

type of the process largely determines the type of sensors and actuators used. The interaction between these components and the controlled process is illustrated in Figure 12.

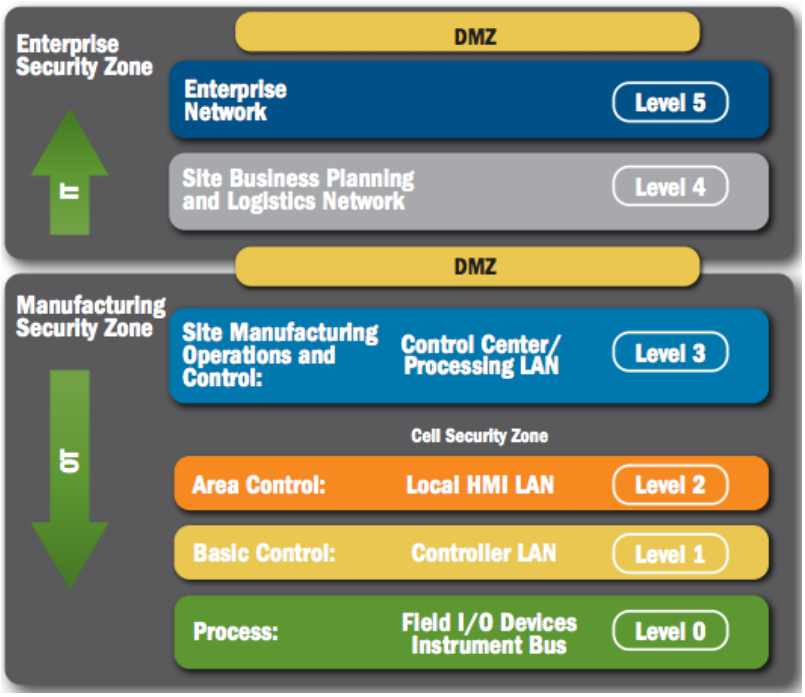


Figure 11. ICS network architecture with security zone segmentation (ICS-CERT & NCCIC, 2016)

One example of a simple system of a sensor, a controller, and an actuator is a thermostat in an air cooling system. A thermostat is a control system used to maintain the temperature near a determined value. In an air cooling system, a thermostat works by adjusting the flow of cool air into a room. If the sensor senses that the temperature is above the determined value, then the flow of cool air will be allowed to flow into the room. Vice versa, if the temperature inside the room is below the determined value, then the flow of cool air will be decreased, or even shut off completely. Different systems employ different kinds of components, but the main principle is similar.

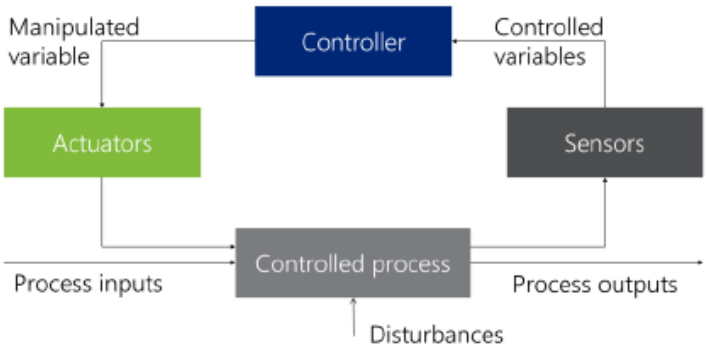


Figure 12. Interaction between sensor, controller, and actuator.

In storage tank operations, the commonly employed sensors are to measure pressure, level, and temperature. These sensors are attached to storage tanks and usually located in different position. For example, the liquid level sensors are typically placed on the top of the tank, while the pressure sensors are typically located on the bottom. The commonly found actuators in storage tank operations are valves and pumps. There are various kinds of pumps and valves. Also, depending on the system configuration, the pumps and valves can be either remotely controlled or can only be controlled on site.

3.3.2.2 Level 1: Controller LAN (PLC, RTU, IED)

The next level of the ICS architecture consists of controllers. The main function of a controller in ICS is to process the received input through a pre-programmed function. Afterward, the output from the controller is sent to an actuator.

There are two different configurations for controllers based on the way they get their input, namely *closed-loop* and *open-loop*. An open-loop system is mainly driven only by an established input (e.g., from operator's input). On the other hand, a configuration is called closed-loop when a system receives feedback from the resulting output of the system itself as an additional input. Thus, in addition to a defined input, the controller also gathers information from the resulting output from the previous process cycle (i.e., feedback). The controller receives feedback from a sensor. In the case of an open-loop configuration, the system may work without the presence of any sensor component. The illustration of open-loop and closed-loop control are depicted in Figure 13. Moreover, a controller works by repeating the same process cycle continuously. This loop of processes works with a cycle time ranging from milliseconds to minutes. The whole continuous process of receiving information from a sensor to making treatment through an actuator is called *feedback control*, or *feedback control loops*.

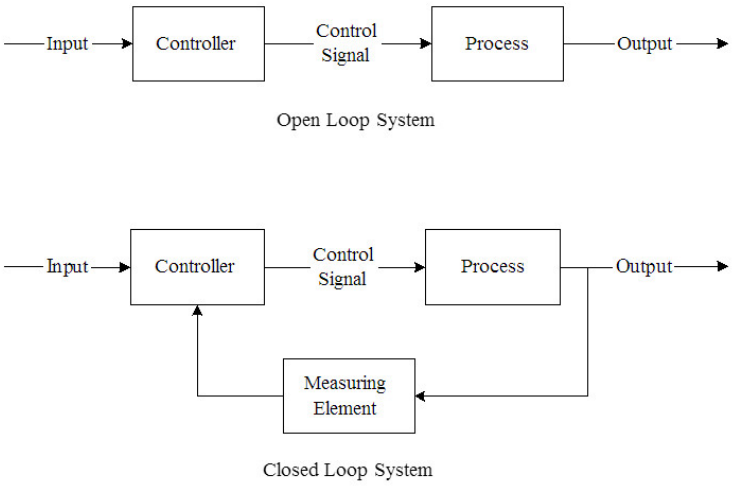


Figure 13. Illustration diagram of open-loop and closed-loop configuration.

One term that is often brought up in a discussion of ICS controllers is the *Programmable Logic Controllers* (PLC). As the name suggests, PLC is a type of controller that encompasses various control components used in various industrial processes, including manufacturing, distribution, and others. One of the main functionalities of PLC is to provide local control over a process using feedback controls. Providing local control also indicates PLCs are placed in areas where the condition of the environment is often harsh. That is why most PLCs are physically hardened to ensure they survive the harsh environment. Also, in addition to being able to connect with sensor

and actuator components, PLCs also have the capability to connect to a workstation on a higher level of ICS architecture.

Another type of equipment that can perform as a controller is the *Remote Terminal Units* (RTU). Historically, RTUs lacked the capability to control other components. The main functionality of an RTU was to transmit measurement data from a remote site to the central control station. Hence, RTU is also known as Remote Telemetry Unit. Some RTUs these days have been equipped with PLC-like capabilities, which allows an instruction to be stored locally inside the RTU. RTUs are often found in SCADA implementations. The ability to function as telemetry and communicate over a limited bandwidth have made RTU an ideal control for remote sites. A large SCADA system may employ several hundred RTUs. These RTUs periodically send measurement data related to each remote site to the control center.

3.3.2.3 Level 2: Local Human-Machine Interface (HMI) LAN

Human-Machine Interface (HMI) can be described as a software and hardware in which information from various subsystems or control components are aggregated and displayed to an operator. HMI, often referred to as a control panel, usually shows information regarding the plant in a schematic diagram of the system it controls. Moreover, some HMIs also allow an operator to send a command to the controllers. For example, in a storage tank system, a symbol of a pump can show whether the pump is running or not, and a gauge symbol can indicate the amount of liquid in a particular tank. Often the depiction of connectivity between components (e.g., pipes between tanks) also present. The operator can interact with the interface, for example, to turn a pump on or off. In this particular layer, the HMI is located on the site to allow local control of the equipment.

Figure 14. Human-machine interface for a SCADA system.

3.3.2.4 Level 2.5: SCADA and DCS

SCADA and DCS are two systems that are encompassed by the broader ICS term. Supervisory Control and Data Acquisition (SCADA) can be defined as a system where geographically dispersed components are supervised and controlled from a centralized site. Typically, a SCADA system is composed of a control center, several geographically dispersed field sites, and a communication system to allow communication between the control center and the field sites. These dispersed field sites are equipped with RTUs to transfer field information to the control center where the data is processed and displayed to the operator. This configuration allows efficient control of a geographically large system. A few examples of SCADA implementation are water distribution system and rail network system.

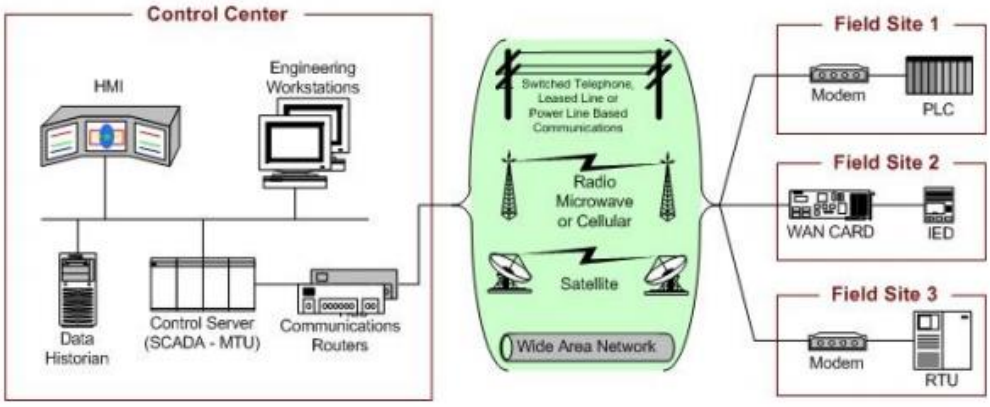


Figure 15. General layout of SCADA system (Stouffer et al., 2011)

On the other hand, Distributed Control System (DCS) refers to discrete subsystems of a localized process that are being controlled by a centralized supervisory computer. Features and functionalities of SCADA and DCS tend to be similar. One key to differentiating SCADA system from DCS is the inclusion of geographically remote or distant sites. A question might arise regarding the exact definition of 'distant' in the previous statement. According to Bailey and Wright (2003), 'distant' can be defined as such a distance between the control center and field sites where direct-wire control would be impractical. Therefore, wireless communication systems are often found in SCADA systems. On the other hand, while SCADA systems tend to be used in a geographically dispersed system, DCS systems are more likely to be employed in a localized area. In DCS systems, the data acquisition and control functions are performed in a distributed manner by number units of controllers that are located nearby to where the main process is done. One example of DCS is a chemical process plant.

Regarding the ICS architecture by ICS-CERT and NCCIC (2016), SCADA and DCS encompass Layer 0, 1, and 2. However, it important to mention there are variations in the definition of SCADA and DCS as well as variations in the composition of the components. For example, Mittal et al. (2017) describe SCADA similarly to ICS-CERT and NCCIC (2016) except that the former also includes the manufacturing zone (Level 3) into SCADA. Another definition of SCADA is presented by Ahmed et al. (2012) in which they describe SCADA as a system composed of all layers from controller layer (Level 1) up until the Internet DMZ layer (Level 5). The main point is there are more than a single definition of SCADA, and a careful approach must be taken when mentioning SCADA systems. The present study will adopt the description of SCADA from ICS-CERT and NCCIC (2016) for consistency purpose.

3.3.2.5 Level 3: Manufacturing Zone

The third level is the manufacturing zone, or also known as the operation zone. A control center for a SCADA or DCS system is usually located on this level, which is why a majority of control and supervisory activities are done at this level. Some of the main components on this level are HMI, ICS server(s), historian server(s), and engineering workstation. In addition to HMIs in field sites, HMIs are also present in this level as part of the control center. This level also comprises several servers that connect to the lower level components, for example, to acquire data from those components. A historian is also a common part of a control center. A historian is a software that records data from various devices in the system into a database. The data in a historian can be used for later analyses. Another main component is the engineering workstation, which is used by engineers to specify processes configuration. Some examples of HMIs from various vendors are

Siemens' SIMATIC WinCC, Wonderware InTouch, Rockwell Automation's FactorTalk View SE, and General Electric's CIMPLICITY.

This level is considered as critical area due to the presence of control centers, which is critical to the operation of the field devices (ICS-CERT & NCCIC, 2016). Another critical point is because this level is the end of the industrial networks before it is connected to the business networks. For safety purpose, a DMZ level is added between this level and the level above (i.e., the Enterprise Zone).

3.3.2.6 Level 3.5: Demilitarized Zone (DMZ)

A DMZ (demilitarized zone) is a term derived from the military domain. In the military, a DMZ represents an area between two states where military operations are not allowed. In computer security, a DMZ represents a subnetwork that acts as an intermediary between a secure network and an untrusted network (ICS-CERT & NCCIC, 2016).

This DMZ sometimes also referred to as the Operation DMZ to differentiate it from Internet DMZ on the higher level. In this level, the secure network is the Manufacturing Zone (Level 3), and the less trusted network is the Enterprise Zone (Level 4). The former belongs to the industrial network, and the latter belongs to the business network. The implementation of DMZ ensures that there is no direct connection between these two networks. In the case of a cyberattack, a potential attacker might get access to servers in DMZ. However, the actual servers where the data is stored are safe. Moreover, the connection between DMZ and the Manufacturing Zone is usually equipped with a firewall[9]. Firewalls may dictate which communication traffic between the two levels are allowed, thus helps secure the Manufacturing Zone from external threats.

3.3.2.7 Level 4: Enterprise Zone

The Enterprise Zone is the level where all the corporate IT systems are located. The Enterprise Zone is often called business network, or corporate network. This level may include components of IT business system, such as enterprise desktop and business servers. Software such as Enterprise Resource Planning (ERP) and a Decision Support System (DSS) might also belong to this level. As a part of the business network, this level is considered less secure when compared to the other levels.

3.3.2.8 Level 5: Internet Demilitarized Zone

The final level in the ICS architecture is the Internet DMZ. The Internet DMZ acts as the barrier between the Enterprise Zone and the Internet. Some of the components on the Internet DMZ level are web servers and email servers, which might need to be regularly accessed by employees from outside the company's network. Similar to the DMZ between Level 3 and Level 4, firewalls are also utilized to help protect the connection between the Internet DMZ and the Enterprise Zone.

3.3.3 Implementation and Utilization in Chemical Plants

The operations and activities which carried out in chemical plants and the typical components that compose ICS have been described in the previous sections. This section continues with the description of how various ICS components are involved in those operations and activities to give a better picture how cyberattacks to help better understand how cyberattacks can affect industrial processes and what the potential impacts and consequences of such cyberattacks.

In chemical plants in general and storage tanks in particular, DCS and SCADA have become the commonly found form of ICS implementation. The use of SCADA can be understood considering

[9] Firewall is a computer network security component that act as a safety screen to help filter hackers or malwares. A firewall is usually implemented as a barrier between a more secure internal network and an external network such as the Internet.

the advantage of remote supervisory and control of dispersed assets in such facilities. DCS is used to control production systems typically found in processing facilities. DSC works by supervising a number of smaller processes which are coupled as part of a bigger production process. Although these concepts are different, their implementations are often hybrids between the two, hence blurring the difference in their real-life implementation (Knapp & Langill, 2014; Stouffer et al., 2011). Both SCADA and DCS are considered as a generic architecture or a conceptual design of ICS components. Hence their implementations might vary from one to another which depend on various factors, such as the type of facility and the type of chemical processes in the plant. However, there are some major components or modules which are typically found in ICS implementations in every chemical facility.

Sensor equipment is one type of component that is always present in both ICS implementations, either in a chemical plant or other types of facilities. As described in Subsection 3.3.2, sensors are an essential building block for a control system. Of the various types of sensors, some of which often appear on ICS implementations in chemical plants such as temperature sensors, flow meter/rate sensors, pressure sensors, radar gauge sensors to measure tank volume, and sensors for warning alarms (e.g., overfill prevention sensor).

Other commonly found components are the valves and the pumps. The pumps and valves are part of the actuator components, and both of them serve an essential function in transferring chemical liquids or gases from one component to another. Most of the pumps and valves that can be found today have functionalities that allow them to be controlled remotely. Remotely controlling these equipment saves time and effort since pumps and valves are typically dispersed throughout the complex facility. Moreover, pumps and valves can also be operated automatically, which partly enables process automation (i.e., feedback control systems).

The next group of components is the RTUs (Remote Terminal Unit) and PLC (Programmable Logic Controller). RTUs collect data from the remote devices and send it back to the master station, while PLCs function to control the actuators (i.e., pumps and valves) based on the predetermined instruction and inputs from sensors. Nowadays, most RTUs also possess PLC’s like functionalities that enable them to perform as the control unit. In SCADA systems, RTUs allow the plant operator to receive data from remote gauging devices and also to send an instruction to the pumps and valves. RTUs are less common in DCS implementation.

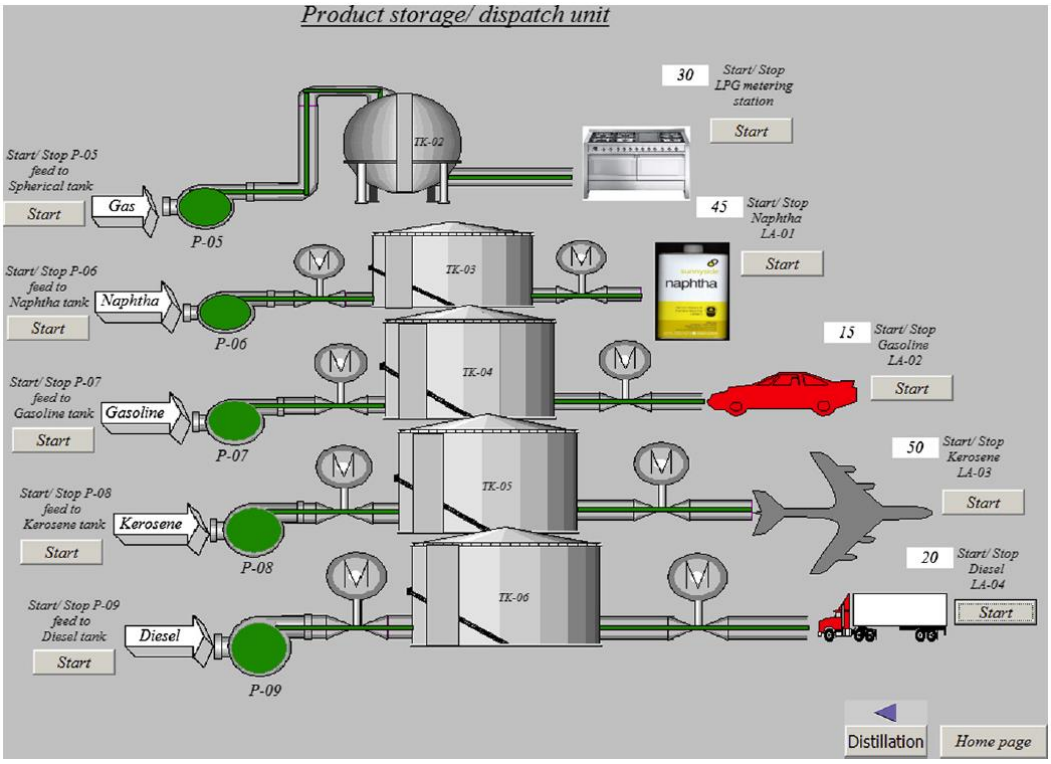


Figure 16. Example of SCADA interface (Morsi & El-Din, 2014)

Another important component of ICS is the HMI (Human-Machine Interface). HMI is the interface that handles interaction between operators and the system. In ICS, HMIs function as a dashboard that displays plant-wide information to the operators, typically in a near real-time fashion. Information such as tank level, the state of the pumps and valves, and the alarm status are usually displayed in HMIs. Moreover, HMIs also allow system configuration and controls over industrial processes in process plants. An example of an HMI graphical interface is presented in Figure 16.

In conclusion, SCADA and DCS are types of ICS that are widely implemented in chemical facilities. SCADA implementations in process plants allow supervisory and control actions to be performed from a large distance while DCS provides supervisory and control over multiple, integrated sub-processes. Implementation of SCADA and DCS system provides several advantages, such as increasing efficiency, quality improvement, improvement in safety by removing humans from hazardous activities, etc. However, the integration of remote supervisory and control capabilities also presents another unexpected challenge in securing the system against threats from the cyberspace. In the next chapter, a more detailed discussion about the cybersecurity of chemical facilities in the light of ICS implementations is presented.

3.4 Cybersecurity of ICSs in Chemical Plants

Cybersecurity in chemical plants has become a critical issue since the significant adoption of ICS in these facilities. The capability to control critical industrial processes remotely using a computerized system has enabled more effective and efficient ways to manage these process, but at the same time also allowed malicious actors to inflict harm to these processes by exploiting vulnerabilities within the system. Hence, from the security standpoint, the adoption of ICS by industrial facilities also calls for cybersecurity practitioners to expand from securing information assets to protecting industrial processes from turning into physical disasters. In the following section, some aspects related to cybersecurity of ICS in chemical plants are described.

3.4.1 History of Cybersecurity-Related Incidents in Process Industry

Chemical and process plants have been subject to cyberattacks for the past few years. Among different kinds of cyberattacks, cyber espionage is the most frequent attack. The existence of valuable proprietary information (e.g., intellectual properties) makes these facilities an attractive target for cyber espionage from various kinds of cyber attackers. There have been several documented cyber espionages on chemical plants where the attackers were stealing intellectual property-related assets. In addition to cyber espionage, (cyber) sabotage is another kind of cyberattack that is equally or even more dangerous. While cyber espionage attacks mostly result in an economic loss, sabotage may result in both an economic loss and loss of life. Sabotage on chemical plants not only result in halt of operation, but also possibly lead to a physical damage. Physical damages from cyberattacks have been documented to happen in the past and remain one of the most discussed cybersecurity issue to date.

One of the earliest known incidents of successful cyberattacks against industrial facility allegedly goes back to the cold war era. In 1982, a former Soviet Union is believed to have been a victim of a cyberattack when a Trojan horse was deployed to attack the control system of the Trans-Siberia gas pipeline (Reed, 2005). The Trojan horse caused the components in the pipeline to fail, and the result was a massive explosion to the pipeline.

Stuxnet is arguably still the most notorious example of cyberattacks toward industrial facilities. Commonly regarded as the first cyber weapon ever invented, the worm is specifically designed to attack Natanz uranium enrichment plant in Iran (Langner, 2011). Stuxnet works by spreading and propagating through USB sticks and local network without the need of an Internet connection. In each infected host, it looked for one specific controller with an exact configuration. Once it found the targeted controller, the worm deployed a set of malicious instructions to cause speed fluctuations in the centrifuge, while providing the monitoring system with recorded system reading to prevent suspicion. As a result, the centrifuge was damaged and the Uranium enrichment facility is shut down for at least one week after the incident. After the first reported infection, Stuxnet is reported to have infected approximately 10,000 similar controllers, mostly in the US, Iran, Iraq, and Indonesia (Exida, 2015).

After the Stuxnet incident, another cyberattack incident toward industrial facility happened in Germany. In 2014, a steel mill suffered from a targeted cyberattack (Lee et al., 2014). It is believed that the attacker first gained a foothold on the system through spear-phishing email which contained a document that was infected with malicious code. Once the internal network is breached, the attacker compromises the plant network (industrial network) and caused damage to several individual components of the control system. The result was physical damage to the furnace due to the inability to shut down properly. So far, there has been no suspect for this attack, and thus the motivation behind the attack remains unclear.

One of the latest ICS cyberattack incidents happened in August 2017 in Saudi Arabia. Sadara Chemical Company, a petrochemical company in Saudi Arabia, was attacked by a cyberattack as part of a string of other cyberattacks (McMillan, 2018; Perlroth & Krauss, 2018). The attack targeted the Schneider's Triconex controller which perform regulatory and safety tasks to prevent catastrophic incidents, such as regulating voltage, temperature, and pressure. The researchers believed that this type of attack is intended to sabotage the plant’s operation and cause an explosion. Since such an attack would result in a disaster, it is fortunate that the attack turned out to be unsuccessful due to a bug in the attacker’s computer code. However, there is a worry from the investigators that the actor behind the attack has fixed their mistake soon after the unsuccessful attempt, and the same method of attack can be followed for other targets which utilize the same type of controller.

3.4.2 Understanding Cyber Vulnerability of ICS

Cybersecurity has developed into a significant issue to ICS in industrial facilities and critical infrastructures. To develop a mitigation solution to this problem, it is important to have a fundamental understanding regarding the security issues in ICS. This section does not go into detail describing the potential vulnerabilities of ICS systems, but more towards exploring the fundamental causes of why such vulnerability exists and some of the challenges in mitigating those vulnerabilities. This direction is taken because describing technical vulnerabilities of ICS would not be in line with the mitigation effort pursued in this work (i.e., suppressing the impact instead of preventing the cyberattack from happening).s

One of several ways to understand the security problems in ICS-based systems is to review the history of ICS and to explore the differences between information technology (IT) and ICS. Despite the increasing resemblance of IT and modern ICS, their characteristics from the security perspective offer less similarity. Understanding the main differences between regular IT and ICS from a security perspective also explains why mitigating cyber risk in ICS requires a different approach.

3.4.2.1 ICS Cybersecurity History

The common IT security issue had never been a major problem for ICS since its first implementation a few decades ago. One of the main reasons for this fact is that ICS equipment and devices were operating in a local network, which is called the industrial network. During this period, the ICS equipment is locally controlled without the risk of external threat. The problem started to arise when the ICS begins to adopt IT capabilities and becomes connected to the business network for some benefits (Hayden et al., 2014; Knapp & Langill, 2014; Stouffer et al., 2011). Business networks are the commonly found networks installed in the office environment, and activities in this network are usually performed using IT equipment and common network protocols. Compared to the industrial network, business network (or corporate network) has been regarded as the less secure network due to several factors, such as its connectivity to the Internet and unrestricted access to email (Stouffer et al., 2011). This developmental direction has made the ICS equipment more accessible to external threat actors, thus places ICS system at a higher risk of being targeted.

Furthermore, even with proper cybersecurity controls in place, some attack vectors, attacks utilizing zero-days exploit or social engineering technique, might still potentially breach the defense mechanisms in place and allow the attacker to gain access to the network. It is evident from the recent incidents, even with the control mechanisms in place, an attacker could gain access to the industrial operation and inflict physical damage upon the targeted facility when equipped with the right amount of skill and resource (Lee et al., 2014; Sanger, 2012). In conclusion, the vulnerabilities of the ICS-based system which emerge from adoption of IT equipment, coupled with the threat originated from the IT network, have resulted in consequences that have never been previously anticipated.

3.4.2.2 Characteristics Differences between IT and ICS: A Security Perspective

Next, this subsection will explain how the different characteristics of IT and ICS affect the security issues of ICS. Table 8 presents some aspects of IT and ICS that are relevant from the cybersecurity perspective.

Table 8. Fundamental differences between IT and ICS (Hadžiosmanović, 2014)

Aspect	Category	Traditional IT	ICS
Technology	*Component lifetime*	3 to 5 years.	15 to 20 years.

Aspect	Category	Traditional IT	ICS
	System operation	Few operating systems.	Common and proprietary operating systems.
	Communication	Common communication protocol.	Open and proprietary communication protocol.
	Resource constraint	Systems usually have sufficient power to support additional security solutions.	Constrained resources to support additional functionalities.
Operation	*Security focus*	Central server and information stored.	Industrial process, and the devices controlling the process.
	Performance requirements	Most important requirements are information integrity and confidentiality.	Most important requirement is information/system availability.
	Time critical interaction	Low/medium requirement for timely interaction.	High requirement for timely interaction.
	Change management	Changes and updates are regularly performed.	Changes and updates need to be thoroughly examined before deployment.

The first point relates to the lifetime of ICS components. Different from IT components that typically have a lifetime between around 3 to 5 years, the lifetime of ICS is around 15 to 20 years, which is significantly longer. From the security perceptive, his characteristic leads to two drawbacks. First, the of lack computational power of the older components often restrict the implementation of security solutions. For example, the computational constraint of PLCs may limit the application of security solution on these components (Hadžiosmanović, 2014). Second, many vulnerabilities are simply resolved by the evolution of technology, such as through the utilization of new protocol, the use of new security standard, and others. These drawbacks are not exhibited by IT components due to their rapid development and evolution.

Still referring to the points in Table 8, the second point includes the performance requirements, time-critical interaction, and change management. The combination of these characteristics has made the patch management in ICS components becomes difficult. For instance, downtime is often required when applying system updates, and in industrial facilities downtime would need to be scheduled days or even weeks in advance. Moreover, updates for ICS related components require thorough testing from ICS experts, security engineers, and IT personnel. All in all, these characteristics prevent system updates to ICS components from being implemented on time, hence potentially leaving vulnerability untreated for a considerable period.

In conclusion, these fundamental differences have critically affected the robustness of ICS against cyber risk, and therefore mitigating security issues in ICS might require a different way than security issues mitigation in IT.

3.4.3 Threat Actors Landscape

The issue of cyber vulnerability in ICS components has been explored in the previous section. However, vulnerability alone is not sufficient to constitute security risks. According to the FAIR (Factor Analysis of Information Risk) concept of information risk, several aspects of the threats are

required for measuring information risk. In this section, the types of actors who pose a threat to the chemical plant are described, which then may provide a clearer picture of the risk of cyberattacks on this facility.

The potential cyber threat profiles of chemical plants can be derived by looking at two points of view: (1) chemical plants as facilities that employ ICS, and (2) chemical plants as critical infrastructures. Firstly, chemical and process plants are known to be one of the industries that utilize ICSs. Stouffer et al. (2011) mentioned some potential threat actors to ICS, including hostile governments, cyber terrorists, malicious intruders, and disgruntled employees. Beyond the group of malicious threat, there are also other types of threat, such as accidental actions by insiders (i.e., operational mistakes) and natural disasters.

The second perspective of threat profiles can be developed by considering chemical plants as critical infrastructures. De Bruijne et al. (2017) have developed a work a list of cyber threat actor archetypes for the Netherlands' NCSC (National Cyber Security Center). From the list, five out of the eleven archetypes are considered as potential threat actors toward critical infrastructures. These threat actor types are crackers, terrorists, hacktivists, state actors, and state-sponsored networks. Descriptions for these threat actors are presented in Table 9.

Table 9. Descriptions of threat actors against critical infrastructures (De Bruijne et al., 2017).

Threat Actor Type	**Description**
Crackers	Crackers is a group of actors that are destroying for fun or looking for platform for showing off their capabilities. Often crackers are also referred to as cyber vandals or script kiddies. The expertise level of crackers is considered between low to medium, and they typically possess low to medium resources.
Terrorist	Terrorists are regarded as ideologically motivated actors which are coordinated through a hierarchical leadership. These actors are also considered to have high expertise, and medium to high resources. However, it is also mentioned no actual attack from terrorist has ever recorded, and there is a lack of data and experience regarding this group actor.
Hacktivist	Hacktivist is highly similar to the terrorist group in the sense that they are ideologically motivated. Hacktivists considered to have low to medium level of expertise. The key characteristic difference between terrorists and hacktivists is hacktivists are more loosely organized and does not operate in hierarchical leadership.
State Actors	State actors are those who conduct secretive cyberattacks toward enterprises, public sectors, or critical infrastructures. The objectives of the attack could be to gain access to strategic information or geopolitically motivated. State actors' expertise and resources level are considered to be medium to high.
State-sponsored Networks	The state-sponsored networks are composed of state-affiliated groups. Their targets include citizens, enterprises, public sectors, and critical infrastructures. The level of expertise is considered medium to high, and the availability of resources is also medium to high.

Moreover, it is also intriguing to see how different motivations of different threat actors lead to the same target in chemical plants. Arguably, not only assets in the facility are in itself valuable for these threat actors, but also the potentially catastrophic impact that entails cyberattacks to these facilities is a motive for some of these threat actors. For instance, valuable intellectual properties stored in these facilities might appeal to some of the threat actors, from the somewhat "tame" crackers to the more dangerous state actors and state-sponsored groups. One might feel fortunate

that threat actors who pursued damage in critical infrastructures, such as terrorist and hacktivist, are among those considered to possess low to medium resources and skill. However, a worrying development has been recently mentioned regarding the possibility of cyber warfare, in which the more resourceful nation-state actors might begin targeting chemical plants to inflict destruction to these facilities (Gertz, 2017; The Washington Times, 2004). This development can only further emphasize the need to mitigate the risk of cyberattacks against critical infrastructure.

3.4.4 Potential Impacts of Cyberattacks on Process Plants

In the previous section, it has been mentioned that there are different kinds of potential threats to chemical plants, where each threat profile is presumably driven by different motivation. In that sense, it can be understood that depending on the motivation, different cyberattacks may yield different impacts. Moreover, the potential impacts of cyberattacks toward ICS in industrial facilities differ from cyberattacks toward traditional IT systems mainly because both deal with entirely different assets: traditional IT deals with information and data, while ICS deals with industrial processes. According to Maryna Krotofil and Gollmann (2013), the cyberattacks toward industrial processes can be classified into three categories as shown in Table 10.

Table 10. Classes of cyber-physical attacks (Marina Krotofil & Larsen, 2015)

Equipment damage	**Production damage**	**Compliance violation**
• Equipment overstress • Safety limits violation	• Product quality • Production rate • Operating cost • Maintenance effort	• Safety • Pollution • Contractual treaties

In addition, Stouffer et al. (2011) developed a list of potential incidents that might arise from malicious actions toward ICS:

- Disruption of ICS operation caused by delay or block of flow of information
- Damaged, disabled or shut down equipment, adverse environmental impact, and/or endangerment of human life from unauthorized changes to instruction, commands, or alarm threshold
- Adverse effects from sending inaccurate information to system operators
- Various adverse effects as result of attacks to ICS software, either through malware or modification to configuration settings
- Endangerment of human life from safety system interference

From the two lists, it can be seen that physical damage is recognized as one of the potential impacts of cyberattacks on control systems. Some of the recent incidents, such as the Aurora generator test in 2017 (Zeller, 2011), the Stuxnet malware (Langner, 2011), and the German steel-mill incident (Lee et al., 2014), have demonstrated the capability of cyberattacks to destroy components in industrial facilities. With regard to cascading effects, considering the interdependent and interlinked components in industrial facilities, it can be understood that any incident in these facilities may potentially lead to a cascading event. Accordingly, the potential impact of cyberattacks against hazardous facilities has been recognized as possible trigger to cascading accidents (Moreno et al., 2018). Moreover, with considerable resource and highly skilled actors (i.e., state-sponsored and state actors) among the potential threat profiles, the possibility of cascading effects to result from cyberattacks cannot be undermined.

3.4.5 Network Segmentation

Network segmentation has been recognized as a common practice in both IT networks and ICS networks to increase the security of the system. It can be defined as the attempt or process to structure ICS components into multiple smaller segments. In the present study, the segregated partitions of the network will be referred to as "network segments," or simply, "segments." The following definition of network segmentation is offered by Security Roundtable (2018):

> **Network Segmentation** – Partitioning computer networks into subnetworks with the aim of preventing the spread of cyber threats. The main idea is when a data breach occurs in one of the segments, the attack will be contained within that network segment, and limited from accessing the other parts of the network.

Network segmentation can be implemented as part of the defense-in-depth strategy (Metivier, 2017). The conventional approach to designing network security is to focus on hardening the network perimeter from external threats. However, under the presumption that there is no perfectly secure system, the defense-in-depth strategy emphasizes on building multiple layers on defense that would slow down adversaries even when the first line of defense is breached. Network segmentation is an ideal method for realizing the defense-in-depth strategy due to its capability to create additional perimeters inside the network. Therefore, even in the case of a security breach, the adversaries would still be limited from accessing assets located in different segments.

Network segmentation can be implemented using different techniques and technologies, namely, among others, physical segmentation, logical segmentation, and network traffic filtering. Physical segmentation is a system segmentation method that utilizes separate communication infrastructures for different segments. On the other hand, logical segmentation is implemented logically, e.g., using Virtual LANs (VLANs) or virtual private networks (VPNs). Logical segmentation potentially presents a comparable security advantage offered by physical segmentation, while also provides greater flexibility and a relatively lower cost. Lastly, network traffic filtering provides segmentation by restricting certain parts of the system from communicating with the others.

4 Research Approach

To answer the main research question, the answers to the sub-research questions must be obtained which involve different kinds of approaches. This chapter starts with a summary of the approaches and the corresponding sub-questions which are presented in Table 11. Subsequently, the methods are described in more detail in the following section.

Table 11. Research questions and the corresponding approaches

	Sub-research Question	Research Approach
[SQ1]	How do cyberattack-related cascading effects happen in chemical and process plants?	– Literature study
[SQ2]	How to model and analyze cyberattack-related cascading effects using Bayesian network?	– Bayesian network methodology (Khakzad et al., 2013) – Graph theory metrics (Khakzad & Reniers, 2015)
[SQ3]	What are the factors of ICS network segmentation design that can influence cascading effects in chemical plants? How can these factors contribute to mitigate cascading effects in case of cyberattack?	– Literature study – Risk-based method
[SQ4]	To what extent does the segmentation design modification mitigate the risk of cyberattack-related cascading effects?	– Case Study

4.1 Research Methods

4.1.1 Takeaways from the Literature Review

Briefly summarizing the previous chapter, several key concepts which are essential to answering the main research question have been explored in the literature review. Sub-research question number one (SQ1) and number two (SQ2) have already been answered in the preliminary literature review in the previous chapter. The answer to SQ1 is presented in Subsection 3.4.4 (pg. 43), as the subsection describe the potential impact of cyberattacks toward ICS in chemical process plants. The answer to SQ2 is presented in Subsection 3.2 (pg. 22), in which the use of Bayesian network methodology by Khakzad et al. (2013) to model and analyze cascading effects, and the application of graph theory to indicate the criticality of an accident scenario are described.

4.1.2 Methodology Development

Following the preliminary findings in the literature review, the methods for building the methodology can be defined. Firstly, the third sub-question (SQ3) explores the factors that contribute to the cascading risk of network segmentation designs, and how these factors influence the risk level on the designs. The answer to SQ3 provides the main building block to the development of the risk-based methodology, which answers the main research question. To answer SQ3, the preliminary literature review suggests a more in-depth investigation into the following three aspects is required: the implication of network segmentation to cascading effects, risk analysis for cyberattack-related cascading effects analysis, and the utilization of graph-theoretic metrics to identify criticality in ICS network segmentation design.

First, the effects of ICS network segmentations to cyberattack-related cascading effects need to be understood. The understanding can be achieved through exploration on some fundamental aspects, such as on the application segmentation on ICS network, the mechanism and potential consequences of cyberattacks on ICS, how network segmentation affects cyberattacks on IT and ICS networks, and others. For this purpose, some insights can be gathered from the literature review of relevant studies, whitepapers from private companies engaged in the field of cybersecurity, reports from governmental organizations, etc. Afterward, an understanding of how network segmentations would influence cascading effects which initiated by cyberattacks can be developed. Chapter 5 is dedicated to the exploration and investigation of this subtopic, and specifically, the implication of ICS network segmentation to cascading effects is presented in Chapter 5.2.

Once the implication of network segmentation is understood, the next step is to formulate an approach to analyze the risk of cascading effects while considering the effect of network segmentation. More specifically, a method to evaluate the robustness of network segmentation design against cyberattack-related cascading effects must be developed. For this purpose, a methodology developed by Khakzad et al. (2013) can be employed to model and analyze cascading effects. However, as can be seen throughout Subsection 6.2.1, estimating the risk level for a single network segmentation design can be a lengthy and complicated process. From the decision maker perspective, doing the lengthy assessment to numerous design alternatives repeatedly can be considered time-consuming, and in the larger projects, may even become unmanageable (Khakzad et al., 2016). Because of this, it would not be inefficient to examine all the possible design alternatives with the hope of finding the most robust one. Moreover, producing a few alternative designs without a clear guideline would risk of producing bad alternatives. Eventually, applying the methodology to these alternatives would merely result in the best design among the worst.

As a solution to this problem, a criticality analysis based on graph theory can be incorporated into the methodology to help with the preliminary network design process. Khakzad and Reniers (2015) have demonstrated the efficacy of graph theory metrics to indicate criticality of accident scenarios with regard to cascading effects. The application of graph theory in the methodology would allow an early identification of severe accident scenarios, which would help in producing more robust design alternatives. That way, a more robust design can be produced without having to consider too many alternatives.

Finally, the findings from this exploration are synthesized to develop a risk-based methodology for mitigating cyberattack-related cascading effects. The detailed process of the methodology development is presented in Chapter 6, while the risk analysis using the BN method is described in Chapter 6.2.16.2, and the application of graph theory is given in Chapter 6.3.

4.1.3 Methodology Application to a Case Study

Lastly, the fourth sub-question (SQ4) calls for the application of the methodology to a case study using a realistic ICS network example. The case study is intended to examine the efficacy of the methodology in improving robustness against cascading effects. Moreover, the case study provides

some insights for the future development of the risk-based methodology. The methodology application is presented in Chapter 7.

4.2 Research Flow

Following the methods described in the previous section, for the sake of clarity, the flow of the research can be illustrated as presented in Figure 17.

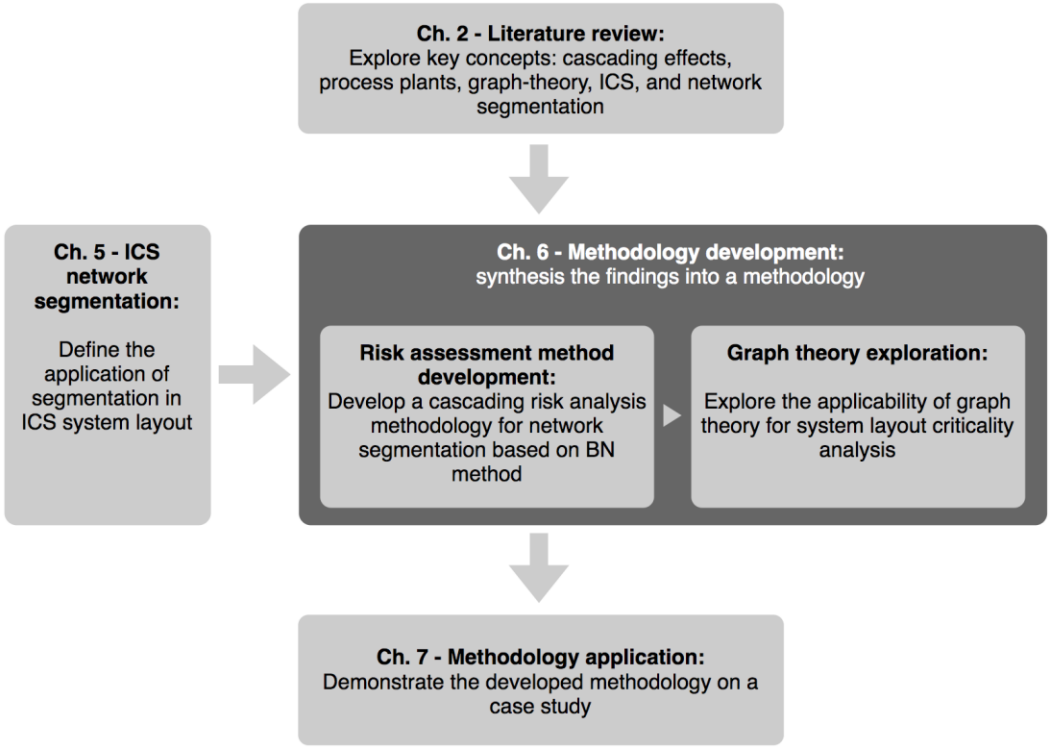


Figure 17. Research flow diagram of the present study.

This page intentionally left blank

5 ICS Network Segmentation

Previously in Subsection 3.4.5, network segmentation has been introduced as a control measure against threats from cyber activities. This section extends the previous discussion on network segmentation by presenting a more extensive exploration of the network segmentation implementation in industrial control systems. Subsequently, network segmentation will be introduced as a means of mitigation for cyberattack-related cascading effects in process plants. The goal of this chapter is to gather as many insights about how network segmentation influences cyberattack-related cascading effects. The insights obtained in this chapter would be used for cascading effects analysis and methodology development in Chapter 6.

5.1 Introduction to Network Segmentation in ICS

The application of network segmentation on ICS is similar to the application of network segmentation in IT in terms of its implementation as well as its purposes and benefits. The similarities can be understood considering the modern ICS systems are essentially industrial systems that achieve IT capability through the adoption of IT components in its system.

The applications of network segmentation in ICS network as a security measure have been mentioned and demonstrated in several previous works. Stouffer et al. (2011) have proposed partitioning ICS network into multiple smaller subnetworks. The basic idea of network segmentation was described as minimizing access to critical information from systems or people who do not necessarily need it while maintaining the daily operation of the organization. The partitioning of ICS into several segments creates perimeters that provide the demarcation for security countermeasures, such as firewalls and proxy gateways. The decision on the segmentation design can be based on several factors, such as management authority, level of trust, and the amount of communication traffic. By implementing the network segmentation on ICS, it is argued that segmentation would make it very difficult for attackers to attain their malicious goals, and at the same time provides containment for the effect of inadvertent errors (Stouffer et al., 2011).

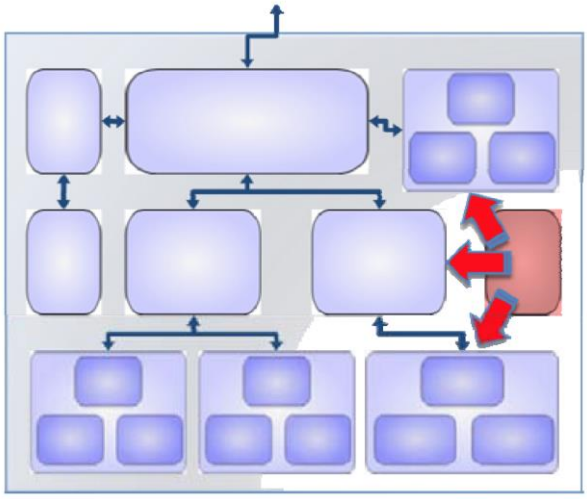


Figure 18. Illustration of a security breach in a segmented system. The segment highlighted in red is assumed to be under security breach. (adopted from Siemens (2008)).

Network segmentation for ICS network has also been proposed by Siemens (2008). In the paper, the segmented parts of the network are referred to as "cells." The goal of segmentation was defined as increasing the system availability through the restriction of failures and security threats to the immediate vicinity. As illustrated in Figure 18, a security breach is assumed to be happening in one of the segments in the system. The key to the network segmentation is that the attackers, having gained access to one of the segment, would have minimal to no influence on components situated in a different segment. Ultimately, the remaining segments can continue to operate normally while the security breach is being treated.

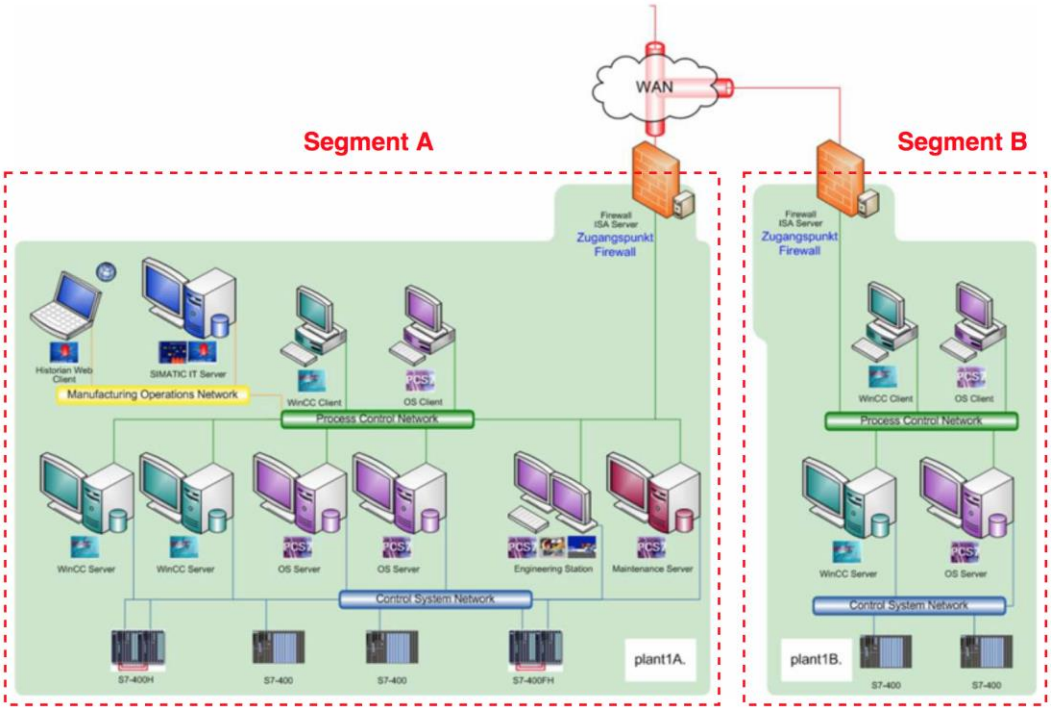


Figure 19. Example of a segmented ICS network implementation (modified from Siemens (2008)).

The implementation of ICS network segmentation can also be observed from the network design perspective. Clearly, different systems are composed of different components. The difference in composition coupled with other factors, such as difference in purpose or technical limitations, encourages the variation in the design of network segmentation to a certain degree. For instance, due to a certain limitation, the design of network presented in Figure 19 can be altered to support a different communication mechanism as shown in Figure 20. On the one hand, these examples show how one factor could force a change in the network design, and on the other hand exhibit a variation of network segmentation designs of an example ICS network.

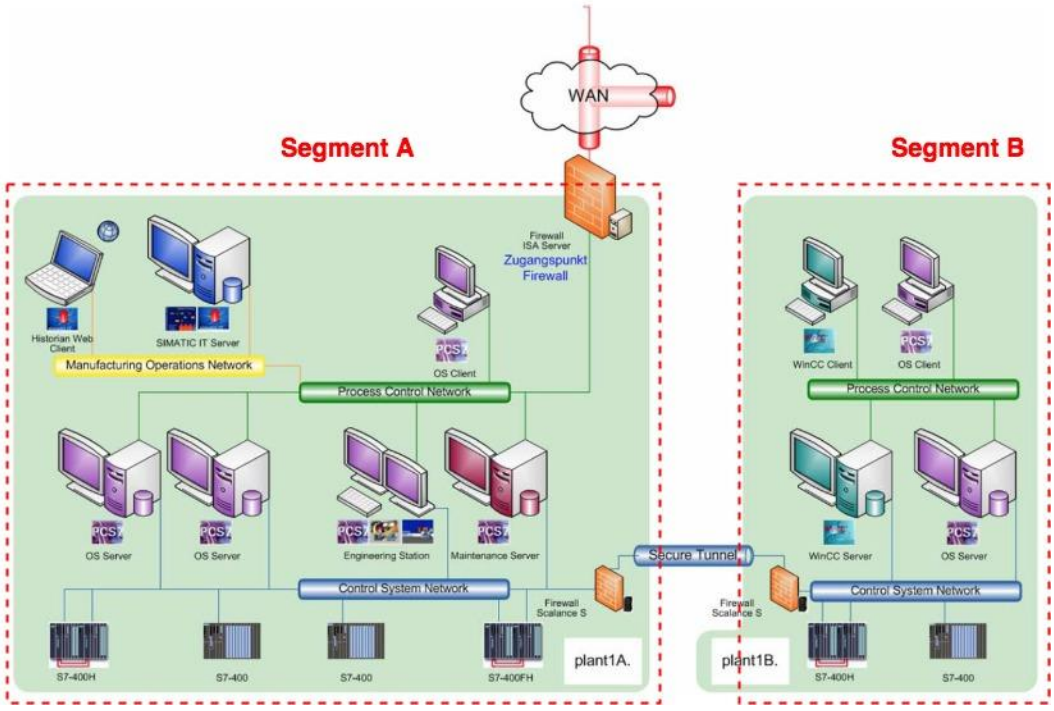


Figure 20. A variation of network design from network in Figure 19 (modified from Siemens (2008)).

5.2 Network Segmentation for Cyberattack-related Cascading Effects Mitigation

5.2.1 How Network Segmentations Mitigate Cyberattack-related Cascading Effects

For the present work, network segmentation is proposed as a technique to mitigate the risk of cyberattack-related cascading effects. It has been mentioned that network segmentation limits the consequence of cyberattack by creating separation between groups of components, resulting in segments of components. These partitioned segments will perform as a defense mechanism should any component within the segment is infiltrated by an attacker. However, it is still important to note that a certain amount of damage can still be inflicted within the attacked segment. To better understand how network segmentation conceptually works in cyberattack-related cascading effects mitigation, see the bowtie diagram illustrated in Figure 21.

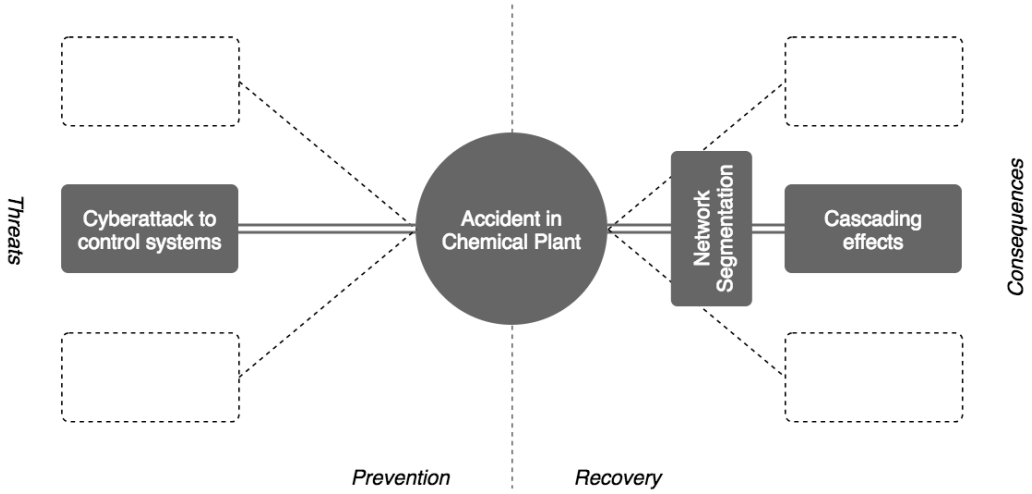


Figure 21. Bowtie diagram illustration of network segmentation for cyberattack-related cascading mitigation.

To the best of our knowledge, network segmentation has never been used for any cascading effects mitigation attempt, though it has been utilized for other reasons and purposes. For example, network segmentations have been implemented for increasing network performance, security improvement, or due to physical constraints (Genge & Siaterlis, 2012). Accordingly, the components in segmented networks can be structured and grouped differently according to the objective of the segmentation. For the network segmentation with security purpose, the most common implementation is to segregate the components according to the architecture of the network. For instance, the reference architecture depicted in Figure 10 can be used as a guideline for how the network can be segmented.

In the present work, the proposed segmentation strategy focuses on partitioning the field devices, which are the ICS components of Level 0 in the ICS-CERT and NCCIC reference architecture (see Figure 10). These are the components that directly interact with the physical processes in the process plants. The focus on ICS components can be understood considering the misuse of this components in critical infrastructures potentially causes fire or explosion, which subsequently may trigger cascading effects. Moreover, looking from the network design perspective, it can be said that the typical approach aims to segment the network "vertically," while the proposed approach focuses the segmentation "laterally." However, it is to be noted that while the proposed approach focuses the segmentation to the Level 0 components, it does not limit the components in other levels from being included.

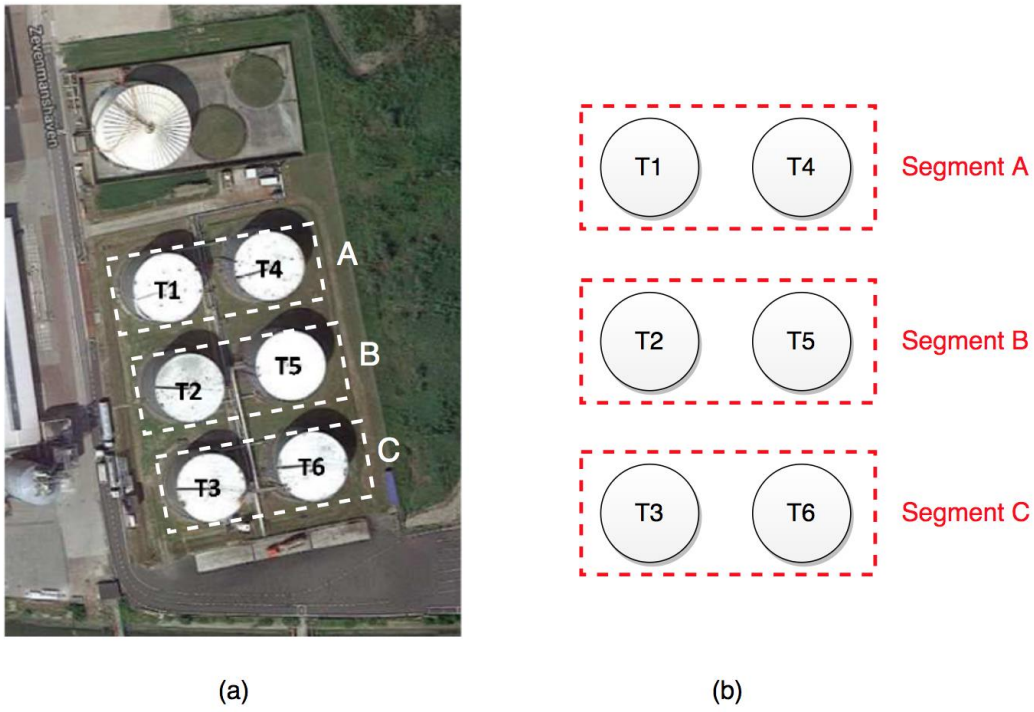


Figure 22. Example of a network segmentation for a storage plant consisting of six storage tanks.

For a better understanding, take an example in Figure 22(a). Assume that the analysis of cascading effects on the example storage plant has already been done, and the resulting outcome suggests to segment the storage tanks as illustrated in Figure 22(b). Next, the ICS components in that process plant can be grouped and segmented according to Figure 22(b) based on their respective storage tank. One example of network segmentation implementation based on Figure 22(b) is presented in Figure 23. However, note that considering that network segmentation can be implemented in different ways, the graph in Figure 22(b) is more of a direction to guide the network segmentation design process, and the realization in Figure 23 is just one of many possible implementations.

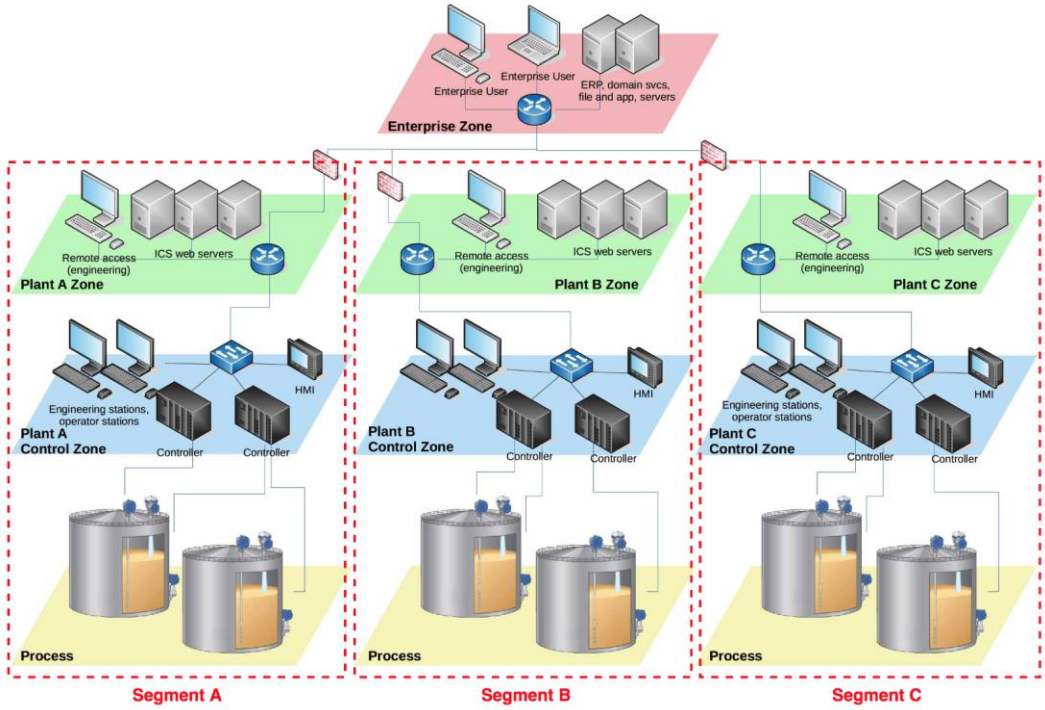


Figure 23. A network diagram example of a segmented storage plant.

Furthermore, it has been stated that the main idea of implementing network segmentation for mitigating cyberattack-related cascading effects is similar to network segmentation for other purposes, which is to limit the potential damage from the adversaries within the segment under attack. Based on the presumption that network segmentation would restrict the access and movement of the adversaries in the network, a network segmentation can be designed in such way that the potential damage from the cyberattacks would impose the least risk of triggering cascading effects. So, for that purpose, a methodology is developed in this work that will examine the segmentation design that exhibits robustness against cascading effects. In Figure 24, it can be seen how a network segmentation works to limit the impact of a cyberattack.

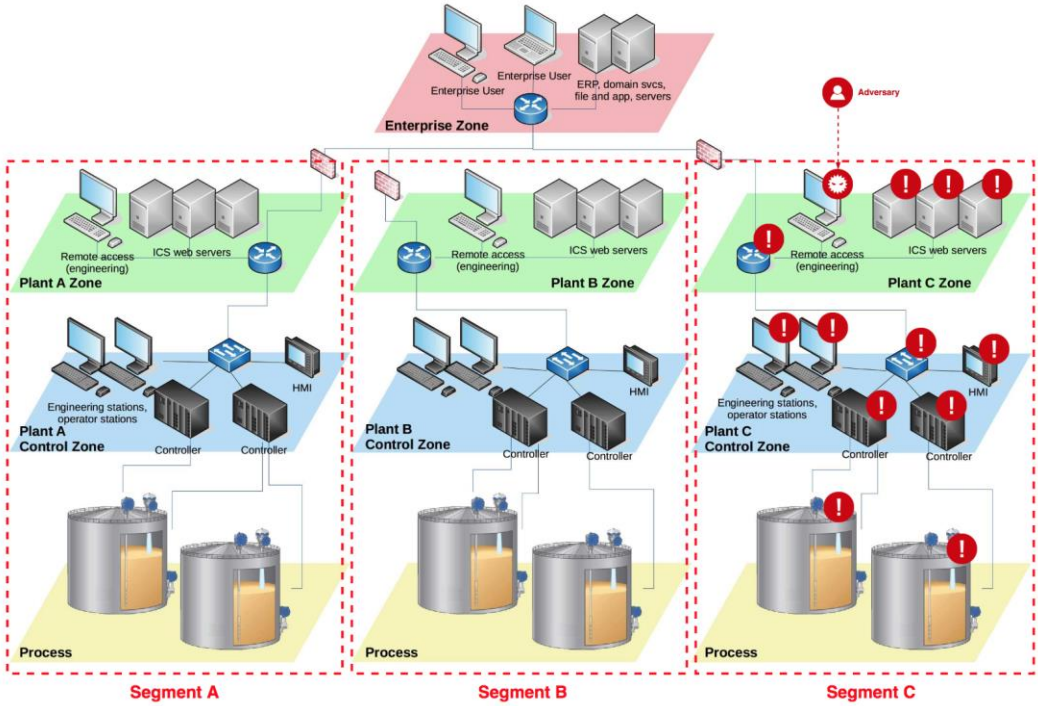


Figure 24. Illustration of a security breach in a segmented system, where the components highlighted with a red exclamation mark are assumed to be at risk.

Moreover, as with the nature of system segmentation, the proposed segmentation rules can be applied in combination with other segmentation rules. For example, Figure 25 shows the proposed segmentation being the subset of the typical segmentation rule. Therefore, the implementation of the risk-based segmentation may provide additional control measures against cyberattack-related cascading effects without sacrificing the benefits from the existing security mechanisms.

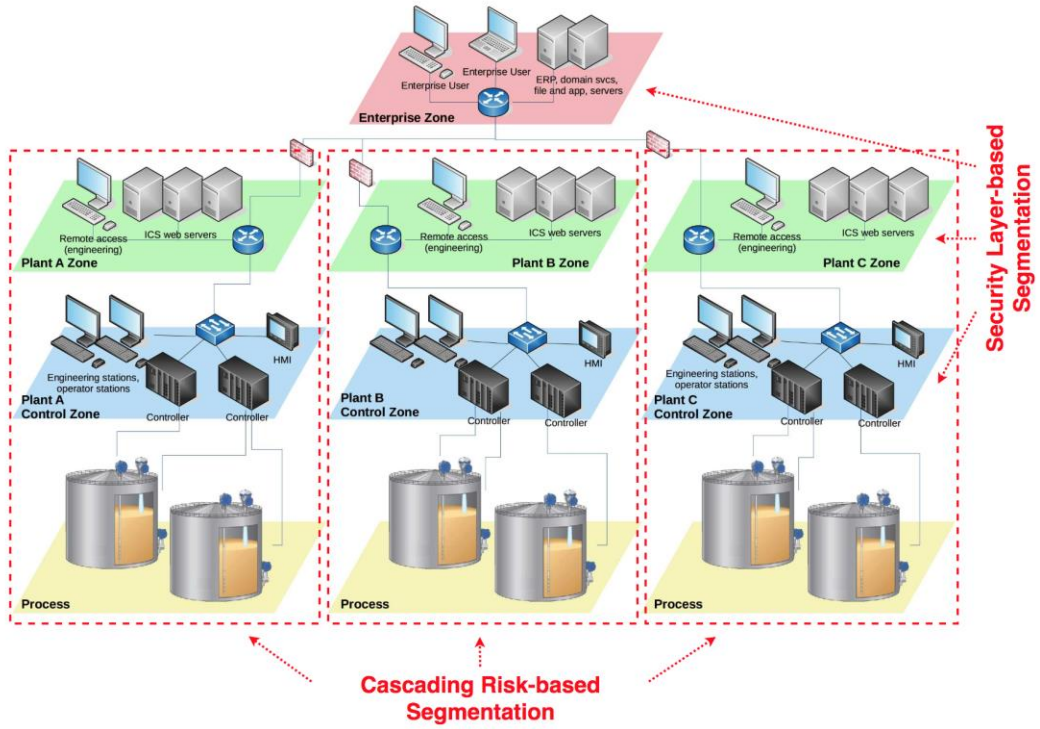


Figure 25. A diagram of network segmentation with both security zone-based segmentation and cascading risk-based segmentation.

5.2.2 Design Aspects Related to Cascading Mitigation

When talking about network segmentation design, or any design in general, it is important to understand that there are several elements that constitute a design. These elements, or often also referred to as design aspects, can be defined as the basic elements which make a design. It is the difference in one or more of these elements that differentiate one design from another. From the literature review, some design aspects of network segmentation are identified:

- The number of segments
- The allocation, distribution, or arrangement of components into segments
- The technology used to realize the segmentation (e.g., virtual segmentation, physical segmentation, etc.)

The present work focuses on two of the design aspects: the number of segments and the allocation or arrangement of the components. It is conceivable that any change in these two design aspects can be represented using the Bayesian network method[10], and hence to a certain degree affect the probability and the risk of cascading effects. Therefore, it can be hypothesized that it is possible to manipulate the design aspects in order to come up with a network segmentation design that yields the least risk of cascading effects.

[10] The Bayesian network method has been introduced as the method for cascading effects modeling and analysis. For more details, see Subsection 3.2.

5.2.3 Bridging Cascading Effects Analysis and Network Design

5.2.3.1 The Gap between Cascading Analysis and Network Design

Using the result from the risk assessment of cascading effects as the main input in designing the segmentation of ICS networks presents its share of challenges. To understand this issue, let us take a step back and review some of the concepts used in this work. Firstly, based on the conceptual framework of this study, it has been understood that cyberattacks toward ICS may result in physical accidents, which may in turn trigger cascading accidents. It is important to note that physical accidents (e.g., leak, fires, explosions, etc.) are the only outcomes from ICS cyberattack that are considered in this study due to their possibility in triggering cascading effects. For an obvious reason, other kinds of outcomes, such as production decline or product quality degradation, are not taken into account.

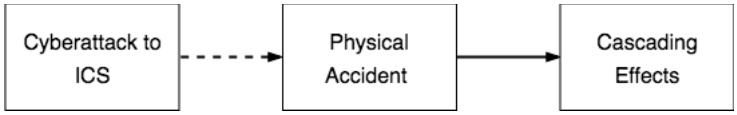


Figure 26. Conceptual framework of the problem in the present study. The dashed line represents a relationship that is not well understood.

Moreover, from the conceptual perspective, there are two relationships in the framework: (1) ICS cyberattacks to result in physical accidents, and (2) for the accidents to trigger cascading effects. The relationship between the triggering accidents and the subsequent cascading effect have been well investigated. There have been a lot of in-depth studies on how primary accidents trigger cascading accidents, including the types of triggering events, the types of escalation vectors, the probability of escalation, and others. Conversely, however, the relationship between cyberattacks on ICS and the resulting physical accidents have not been deeply studied. To illustrate the problem, suppose there are six process units and 25 ICS components in a process plant, determining which component are capable of causing damage to the process units through misuse activities could be complicated. Although make no mistake, the possibility of attacks toward ICS to result in physical accidents not only has been repeatedly established (Moreno et al., 2018; Stouffer et al., 2011), but also has been documented (Lee et al., 2014; Zeller, 2011). The key problem at hand is while physical accidents are among the possible outcomes of ICS cyberattacks, how exactly it may happen can be difficult to describe.

There can be several factors behind this issue. One possible reason is the complexity of process plants. Process plants are complex facilities that are comprised of interconnected components. Thus, it is likely that a change in one component may have side effects on the other components. Additionally, the processes in chemical plants can be highly time-sensitive due to chemical substances in different forms (i.e., liquid, solid, or gaseous) could have an entirely different behavior. Hence, executing the process in plants in a different timing could possibly result in a completely different outcome. Another possible reason is that process plants tend to be highly proprietary. This means the design and components they employ most likely vary from one to another, which implies that the way the plants are controlled is also different (Marina Krotofil & Larsen, 2015). Regarding the problem mentioned previously, this factor may lead to establishing a general method to investigate the relationship between cyberattacks on ICS components and the consequences to be very difficult. All things considered, it is understandable that figuring out how accidents might come up from the misuse of components in process plants requires a deep understanding of each particular plant.

Going back to the main problem, hence determining which components that could contribute to the damage of a particular process unit is a difficult task. That being said, associating ICS components

to the potential accidents is crucial for the present work. It is already mentioned that the result of the cascading analysis would be a physical accidents scenario which presumably has the lowest risk of cascading effect. The network segmentation should follow this recommendation by segmenting the process units according to the accident scenario. For instance, the analysis results indicate that accident involving unit T1, T3, and T5 in a certain tank farm would yield the lowest risk of cascading effect. Hence, the network segmentation should be designed in a way that, in the case of a cyberattack, only units T1, T3, and T5 are damaged as the worst possible outcome. Without knowing how to determine the relationship between the ICS components and the potential accidents in process units, achieving a particular accident scenario through network segmentation manipulation would not be possible.

In summary, the problem that has to be dealt here is that the modeling in the cascading analysis is done using the process units in the plants as the basic components, and the result of the analysis is a recommendation on how these components should be arranged. However, since there is no easy way to indicate which ICS components are related to which process units, taking this recommendation as an input for the network segmentation design is not straight-forward. For the purpose of dealing with this problem, the next section describes the approach employed to manage the disparity between cascading analysis and network segmentation design.

5.2.3.2 Approach for Linking ICS Components to Potential Accidents

Two approaches have been identified to address the relationship between ICS components and potential accidents of the process units. The first approach is the *report-based approach*, in which the relation between ICS components and potential accidents can be established from analyzing the database of past accidents. In process plants and other industrial facilities, the plant owners typically keep a database relating to the incidents that have occurred, which usually include the equipment involved, the causes, the process type, etc. Furthermore, if an accident involving a type of process has occurred in the past, it can be assumed that the accident can be triggered in a similar fashion (Marina Krotofil & Larsen, 2015). By using this assumption, the database of past accidents can also be considered as the database of potential accidents, which implies that misusing the components in a similar way as indicated in the past incident report would result in a similar consequence. By analyzing the potential accidents and the ICS components involved, the lists of related ICS components can be obtained.

However, the report-based approach can be difficult or impossible for various reasons. Arguably, the biggest obstacle is the lack of comprehensiveness of the database. In any process plants, it is highly likely that not all of the accidents that can happen has happened. Therefore, the database may not be sufficient to establish the relation between every ICS component and the potential accidents. Moreover, due to process plants being highly proprietary, most likely these databases cannot be generalized for other process plants, which only further emphasizes the difficulty in pursuing the report-based approach.

Alternatively, the *product flow-based approach* can be pursued. In processing plants, the ICS components (e.g., valves, pumps, gauges, etc.) are connected to either the pipework or the process units. With that in mind, a simplifying assumption can be made: the misuse of ICS components would result in accidents in the process unit where the component is located, or in the nearest process unit within the same product flow if the ICS components are connected to the pipework. Clearly, using such a simplifying assumption would result in a less accurate outcome. To put it differently, the association between potential accidents and the ICS components might not be entirely correct; the misuse of a certain ICS component might lead to an accident that is different than initially suspected. However, looking at the evident difficulty in using the report-based approach, the product flow-based approach is still the better alternative than the two options.

5.3 Potential Drawbacks of Network Segmentation

5.3.1 Overview of the Drawbacks

As described in the previous section, network segmentations offer a potential benefit in term of security. The added security benefit is gained not only through limiting the propagation and access of adversaries, but also from better access control and improved monitoring (Metivier, 2017). Moreover, network segmentation method has also been implemented to improve network availability and performance (Edwards, 2004).

However, despite the added benefits, the application of network segmentation is also accompanied with some drawbacks. For example, either in the case of new system development or transformation of flat (non-segmented) network structure into a segmented one, designing a segmented network requires careful planning which implies extra work required. Afterward, the design must be correctly implemented to ensure the sought benefits can be attained. Furthermore, the application of network segmentation would require additional hardware (White & Bickley, 2001). In some cases, the network resources need to be made redundant for every segment. Therefore, it is clear that there are some costs that come with the application of network segmentation.

Besides the tangible costs such as the design and implementation costs, there are also some intangible costs that must be considered. One of the repeatedly mentioned intangible cost factors of network segmentation is productivity loss (Metivier, 2017; Nicholas, 2017). Network segmentation does not only prevents malicious actors from accessing critical assets but at the same time also creates added procedures and protocols for legitimate users from accessing the same assets. Therefore, the added processes faced by employees would often be regarded as “obstacles” from the usability perspective, which eventually will impact their overall productivity level. Another intangible cost factor comes from the extra work needed to manage and maintain the network (Nicholas, 2017). As previously mentioned, network segmentation often demands the addition of network components, such as servers, switches, routers, etc. From the maintenance point of view, not only that the added components would increase the maintenance effort required, but the separation of these components would also increase the effort required due to the added complexity. In the case of implementation using VLAN, network segmentation might also increase the complexity of processes required for security audit (Zeitlin, 2018).

In conclusion, although network segmentation is a widely recognized method to increase the cybersecurity of a system, it also comes with costs that must be considered. As for the system owners, the objective is to develop a system that is secure from adversaries, while also manageable at the same time (Metivier, 2017).

5.3.2 Calculating the Added Costs

From the organization’s perspective, the drawbacks from network segmentation, either in tangible or intangible form, can be considered as added costs. Hence, the decision on adopting network segmentation should be considered as a trade-off between the security benefit (i.e., reduced cascading risk) and the costs incurred by its drawbacks. For this reason, a method to estimate the additional costs incurred by the application of network segmentation is needed.

Among the two design aspects mentioned in Subsection 5.2.2, the arrangement of components aspect is not indicated to cause any increase in cost. In other words, several designs with different components arrangement (with same number of segments) is not considered to have different cost. On the other hand, increasing the number of segments has been indicated to increase the maintenance cost of the system (Wagner et al., 2017). Therefore, although network segmentation would yield benefit in the form of security improvement, there is a possibility that the increasing maintenance cost may outweigh the benefit of security improvement. To avoid this situation, a cost-

benefit analysis should be conducted during the planning stage. Accordingly, a method to capture the cost incurred by increasing the number of segments must be employed.

It has been mentioned that there are many types of costs related to the drawback of network segmentation. However, accurately estimating all of these costs would be too complex and it would require substantial work. For the sake of simplicity, the present work focuses on the increase in maintenance and operation cost. Table 12 presents the cost factors of IT operation and maintenance in the automation industry.

Table 12. Cost factors of IT operations and maintenance in process automation (adopted from Honeywell (2011))

Operations and Maintenance	
• General maintenance	• Parts availability
• Repair	• Floor space
• Software upgrades	• HVAC/power
• Hardware upgrades	• Proficiency training
• Backups	• Auditing/asset tracking
• Parts replacement	• Downtime

To estimate the increase in costs, a formula proposed by Wagner et al. (2017) can be utilized. The cost function can be used to capture the exponential increase of IT maintenance cost which caused by the addition of segments into the network design:

$$C(env, nsd) = \frac{e^{(N+k)/M} - 1}{e^{k} - 1} \qquad \text{Eq. 9}$$

C being the unit of cost (or cost unit) of IT maintenance for network environment env and network segmentation design nsd, N is the number of segments in nsd, M is the possible maximum number of segments that can be supported, k is a steepness constant ($k = 1, \ldots, 7$), and e is a mathematical constant for the base of the natural logarithm ($e \approx 2.71828$). The steepness constant can be adjusted to represent a more linear increase in cost (e.g., $k = 1$) or the more exponential increase (e.g., $k = 7$). To illustrate, the graph presented in Figure 27 depicts the increase of IT maintenance and operation cost as the number of segments in the network increases.

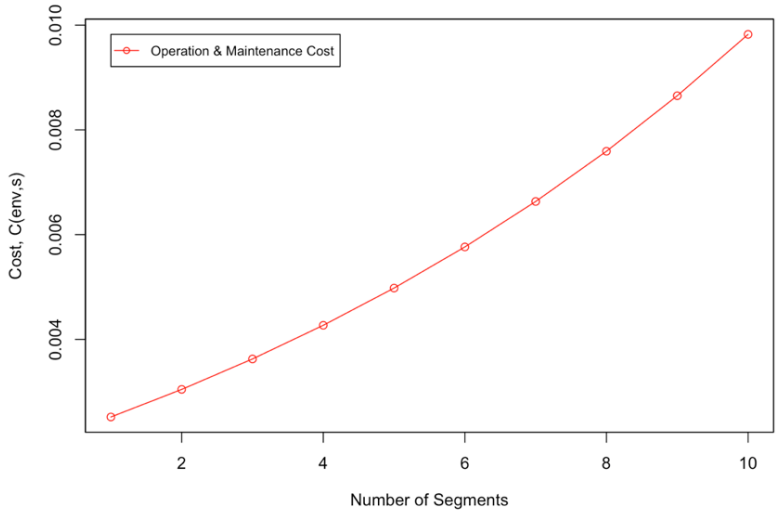


Figure 27. IT maintenance and operation cost function for maximum number of segment M of 10 and steepness constant k of 6

As can be seen, the score of C resulting from the formula is not in currency. To calculate the actual increased maintenance cost, the scale factor of the increased cost unit must be calculated by dividing the cost unit of the segmented system by the cost unit of the non-segmented system. Afterward, the scale factor can be multiplied with the maintenance cost of the non-segmented system to calculate the increased maintenance cost of the segmented system:

$$z = \frac{C(env, nsd_s)}{C(env, nsd_n)} \quad \text{Eq. 10}$$

$$MC_s = z \cdot MC_n \quad \text{Eq. 11}$$

z is the scale factor, MC_s and $C(env, nsd_s)$ being the maintenance cost and the cost unit of the segmented system, MC_n and $C(env, nsd_n)$ being the maintenance cost and the cost unit of the non-segmented system. To conclude, up to this point, a method to estimate the rising maintenance cost has been determined. Later in the next section, this method shall be used in conjunction with the risk analysis method described in Subsection 6.2 to conduct a cost-benefit analysis for network segmentation.

5.4 Feasibility Study: Expert Interviews

To have a better understanding of the applicability of the network segmentation strategy proposed in this study, interviews have been undertaken with two practitioners who work in IT security related fields in chemical manufacturing companies. For the sake of clarity, the organizations in which the interviewees work shall be referred to as Company A and Company B. The discussions were exploratory and mainly revolved around two main points: the current state of ICS networks in chemical and process plants, and whether the type of network segmentation proposed in this study would be a feasible solution from the technical and operational standpoints. It is important to note that the topic being discussed is security sensitive, hence some details about the plant's operation cannot be discussed. Nevertheless, the following are several insights that can be concluded from both interviews.

The first question inquires about the current implementation of network segmentation in interviewees' organization. From the interview, it was discovered that Company A does implement network segmentation for security purpose based on network architecture layers, but does not segment the network further. The interviewee from Company A stated that the typical implementation in storage plants in his company is to manage and control all of the storage tanks in a tank farm from a single control center. In fact, there is an instance of a tank farm where approximately one hundred storage tanks being controlled from a single control center. However, a different situation was found in Company B. The interviewee from Company B described that his company employs both architecture-based segmentation as well as the segmentation similar to the one proposed in this work (see Figure 19).

Moreover, the interviewee from Company A also further explained that network segmentation in this work could not be fully realized in Company A without implementing some changes to the tank farm. There can be several factors that cause this. Based on the interview, the main problem of segmenting a tank farm network is the existence of a shared resource. The shared resource can be explained as a part of the system that needs to be accessed by several other components on the network. By creating a partition on the network, the access to this shared resource will be a lot more limited, and thus will interrupt some operations in the facility. The details of the shared resources cannot be obtained. However, considering hardware components can be easily made redundant in any network structure, it can be presumed that the shared resource is in the form of digital data that is required by various components across the plant for operational purposes.

From the discussions with the practitioners, a few insights can be derived. First, it can be seen that network segmentation has been a standard security measure. Although it was found that the extent of its application may differ, the fact that it is already implemented in both organizations indicates the familiarity of the industry with network segmentation. Second, from the current implementation in Company B, it proves that the network segmentation method proposed in this work is feasible. Third, it can also be presumed that implementing the proposed segmentation method to existing process plants would require a substantial transformation. This implies that the proposed segmentation design is easier to implement in new process plants than the existing ones.

5.5 Key Takeaways

Based on the discussion about network segmentation in the previous section, there are a few important takeaways that can be taken for the cyberattack-related cascading effects analyses in the next chapter. First, network segmentation has been regarded as one of the techniques for limiting the impact of cyberattacks. However, it is important to keep in mind that although the impact of cyberattacks would be "contained" within the segment, the attacker would still be able to inflict some damage within the breached segment.

> **Takeaway #1** – Network segmentation prevents cyberattacks from impacting the whole system. However, it should be understood that a certain amount of damage would still occur.

Next, it has been mentioned that, to some degree, the implementation of network segmentations may be carried out in different ways. Considering this fact, a particular requirement for a certain system can be translated into different forms of segmentation designs. With regard to cascading effects mitigation, it can be inferred that the outcome of cascading analyses can be translated into several segmentation designs. One of the possible implication is the process of cascading analysis can be separated from the segmentation design process of the network architecture. Another possible implication is the outcome of cascading analyses of the methodology to be developed should be independent of a specific kind of implementation.

Takeaway #2 – The outcome of the cascading analyses could be implemented into different forms of network segmentation implementations.

Lastly, the implementation of network segmentation would invoke additional costs, both tangible and intangible. For instance, although intended to block cyber attackers, the effects of network segmentation are also experienced by legitimate users. Engineers and operators who use the system on day-to-day bases would have to suffer productivity loss due to limited access for the sake of security. This and some other costs should be considered when designing a segmentation design.

Takeaway #3 – In addition to risk mitigation benefit, network segmentation also incur costs regarding design and installation, productivity loss, extra maintenance, etc.

This page intentionally left blank

6 Risk-based Methodology Development

In Chapter 5, a deep dive into network segmentation in ICS and how it potentially affects cyberattack-related cascading effects in process plants have been conducted. To start with the development of the risk-based methodology, a method to indicate the risk of cascading effect for segmentation designs must be developed by taking into account the key takeaways from the previous chapter. For this purpose, this study employs a Bayesian network methodology for cascading effects modeling and analysis. As previously explained, the graph-theoretic approach for indicating components criticality is also incorporated into the methodology. Moreover, for the sake of clarity and simplicity, a single hypothetical case study is used throughout the methodology development chapter. In the next section, the development of these approaches and their implementations are described.

6.1 Hypothetical Case for Methodology Development

In this section, the hypothetical case study is described, along with the network segmentation and the attack scenarios of this case study. The plant is a tank farm consisting of six gasoline atmospheric storage tanks, T1-T6 as depicted in Figure 28. All the tanks are identical with a diameter of 33.5 m, a height of 9.1 m, and volume of 8,073 m^3.

Figure 28. Layout of the example tank farm

In accordance with the proposed methodology in this work, the network structure for the tank farm will be separated into several segments using network segmentation. For the present work, the central control is supposed to consist of two segments: Segment A (SgA) and Segment B (SgB). Hence, our goal is to determine network segmentation design that exhibits the most robustness against the risk of cyberattack-related cascading effects.

For the case study in Figure 28, the six storage tanks will be considered as "nodes" for the designing the network segmentation. Nodes can be defined as a part of a system, which can be either a single process unit or a group of process units, whose failure potentially leads to an accident. Division of the nodes into the two segments can be achieved in several configurations. For instance, one possible configuration is to assign T1, T2, and T3 to SgA, and T4, T5, and T6 to SgB. All possible design configurations for the tank farm in Figure 28 are presented in Table 13. However, for the sake of simplicity, the following sections demonstrate the application of BN methodology and graph-theoretic approach for Network Segmentation Design 26 (NSD-26): the SgA comprises of T1, T3, and T4 while the SgB comprises of T2, T5, and T6 (see Figure 30).

Table 13. Every possible network segmentation design for storage plant in Figure 28

Design	Tanks		Design	Tanks	
	SgA	SgB		SgA	SgB
NSD-1	T1	T2,T3,T4,T5,T6	NSD-32	T2,T3,T4	T1,T5,T6
NSD-2	T2	T1,T3,T4,T5,T6	NSD-33	T2,T3,T5	T1,T4,T6
NSD-3	T3	T1,T2,T4,T5,T6	NSD-34	T2,T3,T6	T1,T4,T5
NSD-4	T4	T1,T2,T3,T5,T6	NSD-35	T2,T4,T5	T1,T3,T6
NSD-5	T5	T1,T2,T3,T4,T6	NSD-36	T2,T4,T6	T1,T3,T5
NSD-6	T6	T1,T2,T3,T4,T5	NSD-37	T2,T5,T6	T1,T3,T4
NSD-7	T1,T2	T3,T4,T5,T6	NSD-38	T3,T4,T5	T1,T2,T6

Design	Tanks		Design	Tanks	
	SgA	SgB		SgA	SgB
NSD-8	T1,T3	T2,T4,T5,T6	NSD-39	T3,T4,T6	T1,T2,T5
NSD-9	T1,T4	T2,T3,T5,T6	NSD-40	T3,T5,T6	T1,T2,T4
NSD-10	T1,T5	T2,T3,T4,T6	NSD-41	T4,T5,T6	T1,T2,T3
NSD-11	T1,T6	T2,T3,T4,T5	NSD-42	T1,T2,T3,T4	T5,T6
NSD-12	T2,T3	T1,T4,T5,T6	NSD-43	T1,T2,T3,T5	T4,T6
NSD-13	T2,T4	T1,T3,T5,T6	NSD-44	T1,T2,T3,T6	T4,T5
NSD-14	T2,T5	T1,T3,T4,T6	NSD-45	T1,T2,T4,T5	T3,T6
NSD-15	T2,T6	T1,T3,T4,T5	NSD-46	T1,T2,T4,T6	T3,T5
NSD-16	T3,T4	T1,T2,T5,T6	NSD-47	T1,T2,T5,T6	T3,T4
NSD-17	T3,T5	T1,T2,T4,T6	NSD-48	T1,T3,T4,T5	T2,T6
NSD-18	T3,T6	T1,T2,T4,T5	NSD-49	T1,T3,T4,T6	T2,T5
NSD-19	T4,T5	T1,T2,T3,T6	NSD-50	T1,T3,T5,T6	T2,T4
NSD-20	T4,T6	T1,T2,T3,T5	NSD-51	T1,T4,T5,T6	T2,T3
NSD-21	T5,T6	T1,T2,T3,T4	NSD-52	T2,T3,T4,T5	T1,T6
NSD-22	T1,T2,T3	T4,T5,T6	NSD-53	T2,T3,T4,T6	T1,T5
NSD-23	T1,T2,T4	T3,T5,T6	NSD-54	T2,T3,T5,T6	T1,T4
NSD-24	T1,T2,T5	T3,T4,T6	NSD-55	T2,T4,T5,T6	T1,T3
NSD-25	T1,T2,T6	T3,T4,T5	NSD-56	T3,T4,T5,T6	T1,T2
NSD-26	T1,T3,T4	T2,T5,T6	NSD-57	T1,T2,T3,T4,T5	T6
NSD-27	T1,T3,T5	T2,T4,T6	NSD-58	T1,T2,T3,T4,T6	T5
NSD-28	T1,T3,T6	T2,T4,T5	NSD-59	T1,T2,T3,T5,T6	T4
NSD-29	T1,T4,T5	T2,T3,T6	NSD-60	T1,T2,T4,T5,T6	T3
NSD-30	T1,T4,T6	T2,T3,T5	NSD-61	T1,T3,T4,T5,T6	T2
NSD-31	T1,T5,T6	T2,T3,T4	NSD-62	T2,T3,T4,T5,T6	T1

Further, using two control centers to control the tank farm implies that there could be two attack scenarios against the tank farm; the first attack scenario, At_1, where the control center of SgA is attacked, and the second attack scenario, At_2, where the control center of SgB is attacked. Attacks to SgA or SgB means the storage tanks related to that network segment are at the risk of accident (e.g., major release, explosion). These attack scenarios must be considered when calculating the risk of cascading effects for each network segmentation design.

For the present case, the considered attack scenario is a cyberattack towards the ICS equipment within the tank farm, which may lead to a major release of flammable materials and a pool fire (PF) given ignition (with a probability). Therefore, the impacts of pool fire through heat radiation are taken into account in modeling the potential cascading effects in this example. In the next section, the development and demonstration of the methodology to estimate the risk of cascading effects using the BN method is presented.

6.2 Cascading Risk Calculation

In this section, the development and demonstration of the BN methodology used to estimate the level of cascading risk for network segmentation designs are presented. A hypothetical chemical storage plant depicted in Figure 28 is used to explain how the methodology helps with designing network segmentation.

6.2.1 Bayesian Network Method: Cascading Effects Modeling

Before the risk of cascading effect for the segmentation designs can be calculated, the damage probability of every storage tank must be calculated. To achieve that, the BN methodology developed by Khakzad et al. (2013) is employed. Keep in mind that the following section demonstrate the development and application of the BN method in NSD-26[11].

As previously mentioned, there are two aspects of BNs: the qualitative aspect, which is the structure of BN, and the quantitative aspect, which is the probability aspect (i.e., the Conditional Probability Tables). Firstly, to build the structure of the BN, determining the escalation probabilities is essential. For this purpose, a matrix table consisting of heat radiation from one tank to another can be developed with the help of ALOHA software. Assuming a wind speeds of 2 m/s from Northwest, relative humidity of 25%, and an air temperature of 18 degrees Celsius, the radiant heat intensities are calculated and presented in Table 14.

Table 14. Heat radiation intensity Tj receives from Ti (in kW/m^2)

Ti↓ Tj→	**T1**	**T2**	**T3**	**T4**	**T5**	**T6**
T1	-	38	-	22	-	-
T2	38	-	38	-	22	-
T3	-	38	-	-	-	22
T4	22	-	-	-	38	-
T5	-	22	-	38	-	38
T6	-	-	22	-	38	-

Considering the suggested heat intensity threshold of Q_{th} = 15 kW/m^2 for atmospheric tanks, the values below the threshold are not presented in Table 14 because the possibility of cascading effect for heat intensities below the threshold level is not credible (Cozzani et al., 2005). For illustrative purposes, the storage tanks and the potential escalation vectors can be depicted as a graph as shown in Figure 29.

[11] See Subsection 6.1.

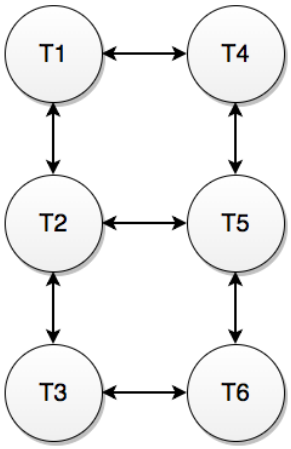


Figure 29. Graphical representation of heat radiation vectors above the threshold. The nodes represent the storage tanks, and the edges represent the heat radiation

Afterward, the primary events for the BN methodology should be defined. For NSD-26, the primary events for attack scenario At_1 occur at T1, T3, and T4, while for attack scenario At_2 at T2, T5, and T6 (see Table 13). The primary units of both attack scenarios are depicted in Figure 30.

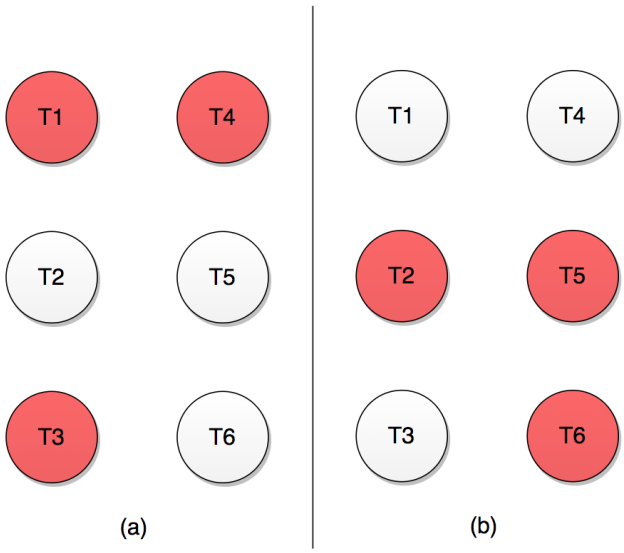


Figure 30. The primary units of NSD-26 in (a) At_1 scenario and (b) At_2 scenario

Based on the primary units, the secondary units can be determined. For instance, take the At_1 scenario (Figure 30(a)) where T1, T3, and T4 are the primary units. Referring to the graph in Figure 29, it is shown that T2, T5, and T6 are at the receiving end of the heat radiation emitted from the primary units, hence T2, T5, and T6 can be considered as the potential secondary units. It is worth noting that the primary units are excluded from the consideration since they are already deemed to be damaged at this point.

To calculate the escalation probability of potential secondary units, the magnitude of escalation vector at the target units must be determined. During this step, the presence of synergistic effects

must be considered. For instance, considering T2 as a potential secondary unit, it is shown in Figure 29 that escalation vectors from T1 and T3 interact and result in stronger heat radiation toward T2.

Based on the values in Table 14, the escalation probability can be calculated using a probit method proposed by Cozzani et al. (2005). The probit value, Y, can be calculated using Eq. 12 and Eq. 13, where Q is the heat radiation intensity (in kW/m^2), V is the tank volume (in m^3), and ttf is the time to failure (s) of a unit exposed to heat radiation. After the probit value, Y, is obtained, the escalation probability, P, can be calculated using Eq. 14, where φ is the cumulative density function, and P is the escalation probability.

$$Y = 12.54 - 1.847 \ln(ttf) \quad \text{Eq. 12}$$

$$\ln(ttf) = -1.13 \ln(Q) - 2.67 \times 10^{-5} V + 9.9 \quad \text{Eq. 13}$$

$$P = \varphi(Y - 5) \quad \text{Eq. 14}$$

The calculation is done using Microsoft Excel spreadsheet software. Table 15 presents the escalation vectors and the calculated escalation probabilities toward T2, T5, and T6.

Table 15. Escalation vectors and escalation probabilities of secondary units for At_1 scenario in in NSD-26

At_1 scenario		
Ti → Tj	**Escalation Vector**	**Escalation Probability**
T1, T3 → T2	76 kW/m^2	9.98×10^{-2}
T4 → T5	38 kW/m^2	3.20×10^{-3}
T3 → T6	22 kW/m^2	5.55×10^{-5}
At_2 scenario		
Ti → Tj	**Escalation vector**	**Escalation probability**
T2 → T1	38 kW/m^2	3.20×10^{-3}
T5 → T4	38 kW/m^2	3.20×10^{-3}
T2, T6 → T3	60 kW/m^2	3.79×10^{-2}

After the escalation probabilities are calculated, the node with the highest escalation probability is chosen to be the secondary unit. For instance, in the At_1 attack scenario T2 has the highest escalation probability (see Table 15), and thus is considered as the secondary unit. Accordingly, causal arcs should be drawn from T1 and T3 toward T2 as illustrated in Figure 31(b), implying that the accident in T2 is conditional to the accident in T1 or T3. Similarly, T3 is chosen to be the secondary unit in At_2 attack scenario for having the highest escalation probability.

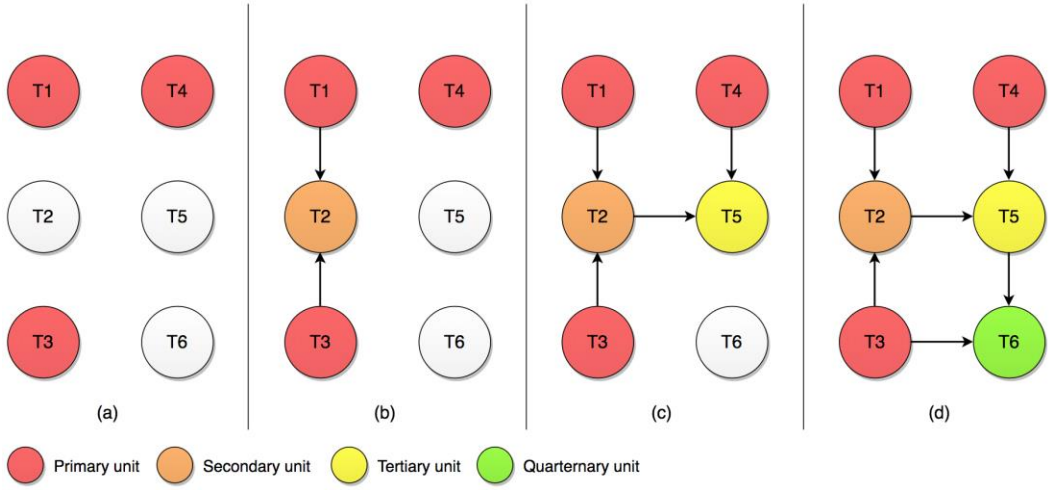


Figure 31. Illustration of Bayesian network development for At_1 scenario in NSD-26

The previous steps are repeated for determining tertiary units: starting with identifying the potential tertiary units using the heat radiation graph in Figure 29, obtaining the heat radiation intensity from Table 14, and using Eq. 14 to calculate the escalation probability, the calculation results are obtained and presented in Table 16. Evidently, T5 is chosen as the tertiary unit in the At_1 attack scenario, and an arc is drawn from T2 and T4 toward T5. However, in the At_2 attack scenario, T1 and T4 have equal escalation probability. Hence, these nodes are considered as the tertiary units in the At_2 scenario, and causal arcs are drawn from T2 and T5 toward T1 and T4 respectively.

Table 16. Escalation vectors and escalation probabilities of tertiary units for At_1 scenario in NSD-26

At_1 scenario		
Ti → Tj	**Escalation Vector**	**Escalation Probability**
T2, T4 → T5	60 kW/m^2	3.79×10^{-2}
T3 → T6	22 kW/m^2	5.55×10^{-5}
At_2 scenario		
Ti → Tj	**Escalation vector**	**Escalation probability**
T2 → T1	38 kW/m^2	3.20×10^{-3}
T5 → T4	38 kW/m^2	3.20×10^{-3}

Whereas all the units in the At_2 attack scenario have been examined, there is still one unit left in the At_1 attack scenario. By following the same steps, the probability for the last unit is calculated and presented in Table 17. The complete structure of BN for At_1 attack scenario is presented in Figure 31(d).

Table 17. Escalation vectors and escalation probabilities of quaternary unit for At_1 scenario in NSD-26

At_1 scenario		
Ti → Tj	**Escalation Vector**	**Escalation Probability**
T3, T5 → T6	60 kW/m^2	3.79×10^{-2}

Up to this point, the qualitative part of the BN (i.e., the structure) has been built, and the quantitative aspect (i.e., the CPTs) need to be developed for all of the six nodes to complete the BN. The CPTs can be developed based on the structure of the BN and the escalation probabilities. For example, the CPT for node T2 is presented in Table 18. Repeating the steps above, the CPTs for the other nodes can be developed.

Table 18. Conditional probability table (CPT) of node T2 for At_1 scenario in NSD-26

T1	**T3**	**P(T2 = Fire | T1, T3)**	
		Accident	**Safe**
Accident	Accident	9.98×10^{-2}	0.90
Accident	Safe	3.20×10^{-3}	0.99
Safe	Accident	3.20×10^{-3}	0.99
Safe	Safe	0	1

Afterwards, using the probabilities in the CPTs, the probabilities of accident for each node can be calculated. In case of a node with a single parent, where X_y is the parent node and X_i is the child node, the probability of accident can be calculated using Eq. 15.

$$P(x_i) = P(x_i|x_y) \cdot P(x_y) \qquad \text{Eq. 15}$$

On the other hand, in the case where there are more than a single parent, such as T2 in Figure 31(b), the probability of accident can be calculated as follow:

$$\begin{aligned} P(T_2 = \text{fire}) = {} & P(T_2 = \text{fire}|T_1 = \text{fire}, T_3 = \text{fire})\, P(T_1 = \text{fire})\, \text{P}(T_3 = \text{fire}) \\ & + P(T_2 = \text{fire}|T_1 = \text{fire})\, \text{P}(T_1 = \text{fire})\, \text{P}(T_3 = \text{safe}) \\ & + \text{P}(T_2 = \text{fire}|T_3 = \text{fire})\, \text{P}(T_1 = \text{safe})\, \text{P}(T_3 = \text{fire}) \end{aligned} \qquad \text{Eq. 16}$$

However, it should be noted that calculating the probability of accident for the primary units requires a different approach. As mentioned earlier in this subsection, the considered outcome of the cyberattack in this example is a major release with a probability of ignition. Accordingly, the probabilities for a cyberattack to result in a major release, and also for a major release to form a pool fire, must be determined. Hence, the likelihood of a cyberattack-driven leakage which may ignite into a pool fire can be calculated as:

$$P(Primary\ pool\ fire|Cyberattack) = P(Release|Cyberattack) \cdot P(Ignition|Release) \quad \text{Eq. 17}$$

$P(Release|Cyberattack)$ is the probability of release due to a cyberattack, $P(Ignition|Release)$ is the probability of the release to meet an ignition source and form a pool fire, and $P(Primary\ pool\ fire|Cyberattack)$ is the probability of a pool fire due to cyberattack. For demonstration purposes, $P(Release|Cyberattack)$ is assumed at 1.0×10^{-1}, and $P(Ignition|Release)$ is estimated at 5.0×10^{-2} (Rew & Daycock, 2004). Hence, the $P(Primary\ pool\ fire|Cyberattack)$ is at 5.0×10^{-3}. Using this assumption, the completed BN for At_1 scenario in NSD-26 is modeled using AgenaRisk software tool (Agena Ltd., 2009), and the result is presented in Figure 32, and the probability of accident of each storage tank in NSD-26 is presented in Table 19.

Table 19. Probability of accident of storage tanks in NSD-26

Network Segmentation Design 26 (NSD-26)		
Storage tank	**Probability of accident**	
	At_1 scenario	**At_2 scenario**
T1	5.00×10^{-3}	1.60×10^{-5}
T2	3.43×10^{-5}	5.00×10^{-3}
T3	5.00×10^{-3}	1.72×10^{-5}
T4	5.00×10^{-3}	1.60×10^{-5}
T5	1.60×10^{-5}	5.00×10^{-3}
T6	3.32×10^{-7}	5.00×10^{-3}

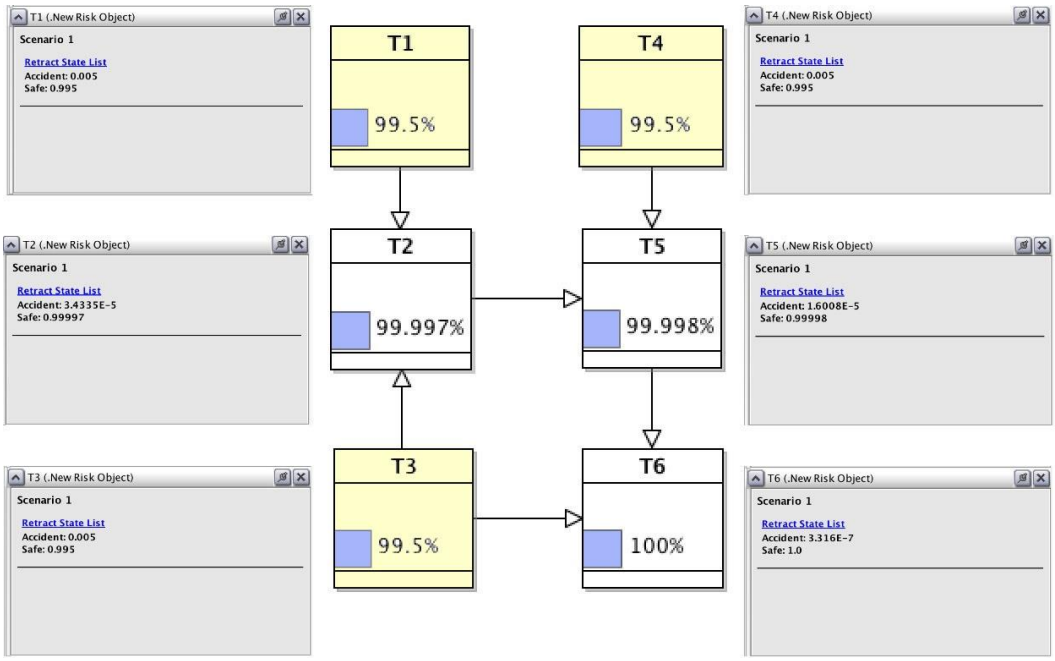


Figure 32. Bayesian-network for At_1 scenario in NSD-26. T1, T3, and T4 are the primary units.

6.2.2 Application of Game Theory for Identification of Attack Scenario Probabilities

So far, a method to estimate the probability of damage for attack scenarios in network segmentation designs has been demonstrated. However, it was explained earlier that the implementation of network segmentation resulted in the emergence of several attack scenarios, which using the BN method produced different risk scores. Before proceeding to the risk analysis stage, a method for consolidating the risk value of several attack scenarios in each network segmentation design must be established.

In the case of adversarial risk analysis, such as the present study, game theory can be employed to improve the outcome of the risk analysis (Cox, 2009). In the context of game theory analysis, the present work can be considered as a simple attacker-defender game. Attacker-defender game, also known as leader-follower game, is a setting where the defenders move first by allocating resource on their defense, and afterward, the attackers deploy a strategy to respond to the defender's strategy with the goal of gaining the optimal outcome. In such an adversarial game, the "minimax" analysis from game theory can be an alternative to assigning arbitrary probabilities to the decisions of the attackers. This minimax analysis describes the strategy of the defender as minimizing the maximum possible damage by anticipating the worst attack scenarios. Therefore, by employing the game theory approach to adversarial risk analysis, a more relevant risk assessment result can be obtained.

> **Minimax** – A strategy in game theory to minimize the maximum loss for the worst case scenario.

Before applying the minimax analysis in this study, several underlying assumptions need to be outlined: the attackers are rational, in complete possession of all information needed for making decisions, and have the capability to compute the pay-offs of every possible strategy. These assumptions often become the point of critics due to its implausibility. However, in a relatively simple situation, such as the attacker-defender games, this criticism is weakened by the fact that the each player would maximize their own payoff (Cox, 2009).

Moreover, in Subsection 3.4.3, the cyber threat actor landscape for chemical plants has been described. With regard to cascading effects analysis in this study, it can be understood that only those actors with the motivation of inflicting damage to the plants should be considered. Based on this argument, an assumption can be derived that the pay-off sought by the attackers is the amount of damage on the facility. In other words, the attackers are assumed to always pursue an attack scenario with the highest risk of cascading accident.

Lastly, for simplicity's sake, it is also assumed that the attackers are only capable of attacking a single segment. Realistically speaking, in a situation where the attacker is highly skilled, and the system is improperly defended, it is possible that the attacker can propagate to the entire system despite the implemented segmentation. However, under such circumstances, it can be argued that the system owners should be dealing with an entirely different issue as the addition of network segmentation would add little to no security benefit.

Following all the assumptions above, the application of minimax analysis to this work can be described as follow. Firstly, different attack scenarios can be identified in the segmentation design alternatives. Next, the outcome (i.e., the risk) from each attack scenario can be estimated by using the BN method. Subsequently, by comparing the risk of each attack scenario, the worst attack scenario can be identified for each segmentation design alternative. By anticipating the worst attack scenario in every design alternative, the system owners should choose a design that yields the least maximum damage (minimax). Ultimately, the chosen design would yield the least risk of cascading effects.

For example, consider an example presented in Table 20, where three design alternatives are being evaluated. Assume that the risk analysis for every segment of each alternative has been done, and the results are presented in the table. Because it is assumed that the attackers always target the most critical segment, the risk score from the segment with the highest risk would represent the risk of the design. For instance, in Table 20, because the risk of cascading effects for Segment B in NSD-1 is higher than that of Segment A, it can be derived that the risk of NSD-1 would be equal to the risk of Segment B. By comparing the risk level of each design alternative, it can be seen that NSD-3 has the lowest overall risk, and therefore can be considered the most robust design alternative. Now that a method to consolidate the different risk value from several attack scenarios has been established, the level of risk sustained in network segmentation designs can be calculated.

Table 20. Example of game theory application during the risk analysis

Design	**Risk**		
	Segment A	**Segment B**	**Overall**
NSD-1	805	990	990
NSD-2	610	1560	1560
NSD-3	**700**	**710**	**710**

Note. The scores presented in the "Overall" column indicate the risk for the segmentation designs after examining all attack scenarios of the design using game theory.

6.2.3 Risk Analysis

The risk of damage for each storage tank is a product of the probability of damage and the value of the tank. For the sake of conciseness, some indirect risks (loss of life, off-site damages, reputation loss, etc.) are not taken into account. Considering that all the tanks are identical, a monetary value

of € 3.1M is assigned to each storage tank (Matches, 2014). For instance, considering the probability of accident in Table 19, the risk sustained by T1 and T2 in attack scenario toward Segment A (At_1) are € 15,500 and € 106.44, respectively. Table 21 presents the estimated risks of damage for the storage tanks in NSD-26 for both attack scenarios.

Table 21. Risk of damage for the storage tanks in NSD-26

Unit	Risk	
	At_1 scenario	At_2 scenario
T1	€ 15,500.00	€ 49.60
T2	€ 106.44	€ 15,500.00
T3	€ 15,500.00	€ 53.15
T4	€ 15,500.00	€ 49.60
T5	€ 49.62	€ 15,500.00
T6	€ 1.03	€ 15,500.00
Total	€ 46,657.09	€ 46,652.35

Furthermore, the risks from each attack scenario should be consolidated into a single value to facilitate rank ordering the segmentation designs based on their risk. As described in the previous section, the game theory analysis can be employed in this case. Based on the assumption that attackers are looking to maximize the amount of damage on the system, and that the attackers are only able to target a single segment, it can be understood that the attackers would pursue an attack scenario with the highest risk in any network segmentation design. Accordingly, the risk of cascading effect for a segmentation design would be equal to the risk of cascading effect for its highest attack scenario. For this example, since the risk level of At_1 is higher than At_2, it can be determined that the risk of cascading accident for NSD-26 is equal to that of At_1.

Table 22. Risk of cascading effects on attack scenarios in NSD-26

Risk		Risk of Cascading Effects for NSD-26
At_1 scenario	At_2 scenario	
€ 46,657.09	€ 46,652.35	€ 46,657.09

Up to this point, the method for estimating the risk level of network segmentation designs has been described. By repeating the steps described above (i.e., building BNs, game theory analysis, and calculating risks), the approximated risk level for other network segmentation designs can be calculated. Subsequently, the risk value between the design alternatives can be compared, and the most robust segmentation design can be determined.

6.3 Design Guidelines for Robust Segmentation Design

In the previous section, the process of examining the robustness of network segmentation designs has been described. As demonstrated, the process of examining the robustness of network designs can be lengthy and complicated. Due to this reason, the number of design alternatives that can be

examined can be very limited. To help improve the effectiveness of this methodology, an additional process can be added prior to the risk-based methodology to ensure that the design alternatives would have good robustness. Afterward, the risk-based methodology can be applied to identify the most robust design among these alternatives.

For this purpose, some design aspects of network segmentation are explored with the goal of developing some guidelines for designing robust segmentation design. The resulting guidelines shall be used in conjunction with the risk-based method to develop the most robust segmentation design.

6.3.1 Graph Theoretic Approach

Criticality of the units based on graph metrics can be a useful criterion to help develop robust segmentation designs. Critical units refer to those units whose failure would contribute the most to the cascading effect in the industrial plant. It have been demonstrated that, by modeling chemical plants as a directed graph, the graph centrality metrics are applicable for identifying the criticality of the units (Khakzad & Reniers, 2015; Khakzad et al., 2016). More specifically, accidents on units with the highest out-closeness score would result in the highest probability of cascading effects, whereas units with the highest betweenness have the largest contribution to the propagation of cascading effects.

For demonstration purposes, the vertex-level centrality of each node for the case study in Figure 28 is calculated. When calculating the criticality metrics for cascading effects analysis, it is important to note the difference in the weight of the edges in the graph. In graph analysis, larger weights represent a longer distance, hence weaker connectivity, whereas in cascading effects modeling, larger weights (i.e., larger escalation vectors or heat intensity) represent stronger connectivity. To manage this difference, the weight of the edges will be presented as a ratio of the threshold value and the value of the escalation vector (Khakzad et al., 2016). For instance, the weight of the edge between T1 and T2 is (15/38) = 0.395. To obtain the centrality scores of the units, the directed graph depicted in Figure 29 is modeled using the igraph software package in RStudio (Csardi & Nepusz, 2006), and the results are presented in Table 23.

Table 23. Centrality metrics for storage tanks in tank farm in Figure 28

Node	Vertex-level centrality			Risk
	Degree	Out-closeness	Betweenness	
T1	2	0.226	1.667	€ 15,550.62
T2	**3**	**0.276**	**6.667**	**€ 15,600.07**
T3	2	0.226	1.667	€ 15,550.62
T4	2	0.226	1.667	€ 15,550.62
T5	**3**	**0.276**	**6.667**	**€ 15,600.07**
T6	2	0.226	1.667	€ 15,550.62

From Table 23, it can be seen that both node T2 and T5 have the largest vertex-level out-closeness score. Using the BN method described in the previous section, the risk values for both T2 and T5 are estimated as € 15,600.07, which are the highest risk value among the other single accident scenarios. This finding conforms to the earlier study, where the largest vertex-level out-closeness score indicates the most severe cascading effect (Khakzad & Reniers, 2015; Khakzad et al., 2016).

That being said, not all factors that affect the risk of cascading effects can be represented by vertex-level out-closeness. For instance, in the case of a tank farm, the volume of the storage tanks plays an important role, which is not represented in the vertex-level out-closeness score. To consolidate the tank's volume into its criticality score, a geometric mean of the vertex-level out-closeness score and the volume can be utilized as shown in Eq. 18.

$$Cr_n = \sqrt{C_{out}(n) \cdot V_n} \qquad \text{Eq. 18}$$

Where n is the node of interest, Cr_n is the modified criticality, $C_{out}(n)$ is the vertex out-closeness, and V_n is the volume. In addition to the vertex-level centrality metrics, the graph-level out-closeness have also been demonstrated to indicate the criticality of nodes in a storage plant (Khakzad & Reniers, 2015, 2018). To calculate the graph-level score, the graph of storage plant can be remodeled based on the scenario of accidents. For instance, to calculate the graph-level out-closeness of single-accident scenarios in T1, T2, T3, …, T6, the graph in Figure 29 can be remodeled according to each accident scenario as shown in Figure 33. The graphs are modeled in the igraph package, and the graph-level out-closeness scores are listed in Table 24. From the scores presented in Table 24, it can be seen that accident in T2 and T5 have resulted in the highest score, which is consistent with the result from the vertex-level out-closeness score.

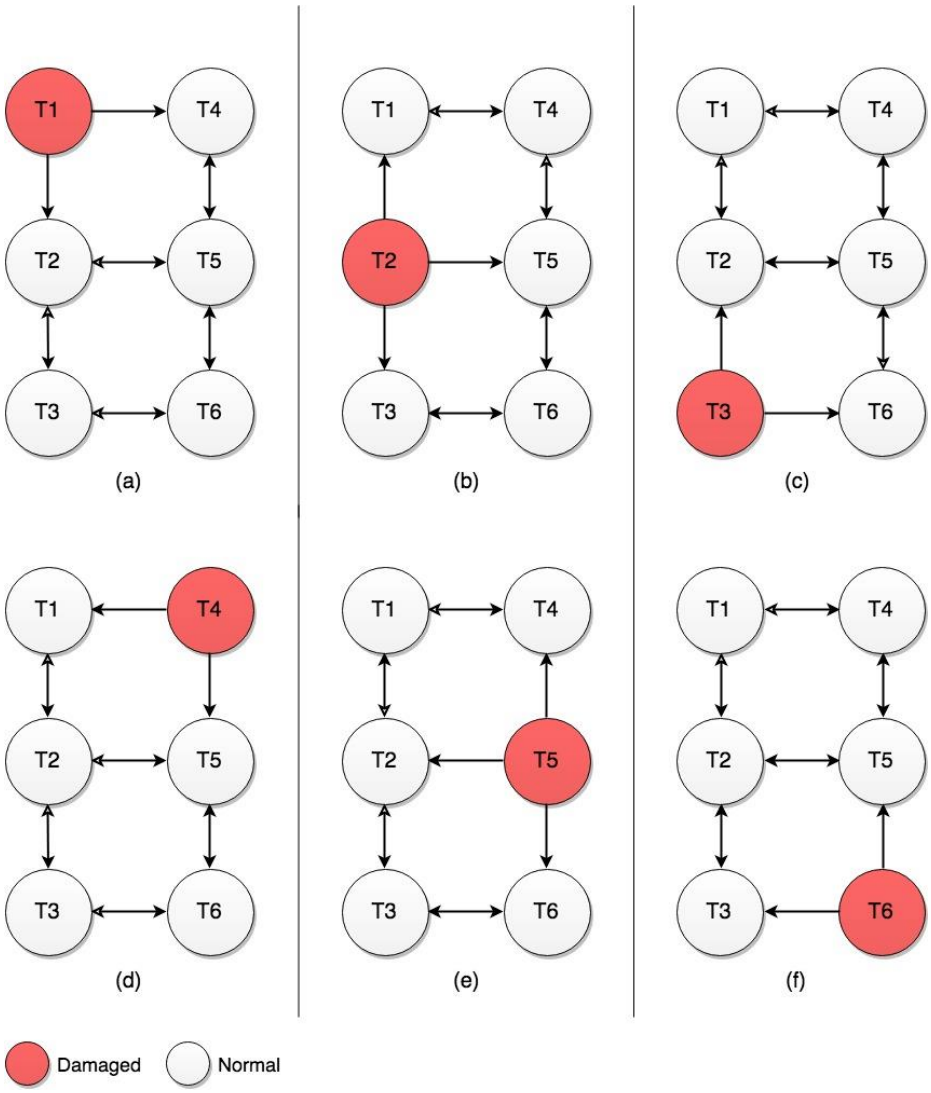


Figure 33. Illustration of cascading effects triggered in (a) T1, (b) T2, (c) T3, (d) T4, (e) T5, and (f) T6.

Table 24. Graph-level centrality for single accident scenarios.

Accident at Node	**T1**	**T2**	**T3**	**T4**	**T5**	**T6**
Graph-level Out-closeness	0.180	0.423	0.180	0.180	0.423	0.180

Moreover, one advantage of graph-level centrality is that it can also be used to indicate the criticality of multiple-accidents scenarios. For instance, it has been shown that double-accidents scenario involving two of the most critical units (i.e., those with the largest vertex-level out-closeness) would result in the most severe cascading accidents compared to any other pairing combination (Khakzad & Reniers, 2018). In the storage plant in Figure 28, the combination of failures in T2 and T5 should result in the most severe accident compared to any other pairs and, hence, the highest graph-level out-closeness score.

For demonstration purposes, consider three double-accidents scenarios as illustrated in Figure 34. To calculate the graph-level out-closeness, the graphs in Figure 34 are modeled using the igraph software package, and the resulting scores along with the risk values are presented in Table 25.

Evidently, the scenario where T2 and T5 are the primary units (Figure 2(c)) resulted in the largest graph-level out-closeness score. Correspondingly, the combination of T2 and T5 also yields the highest risk compared to the other scenarios. Therefore, it is evident that the graph-level out-closeness score can be utilized to indicate the severity of accident scenarios in process plants (Khakzad & Reniers, 2018).

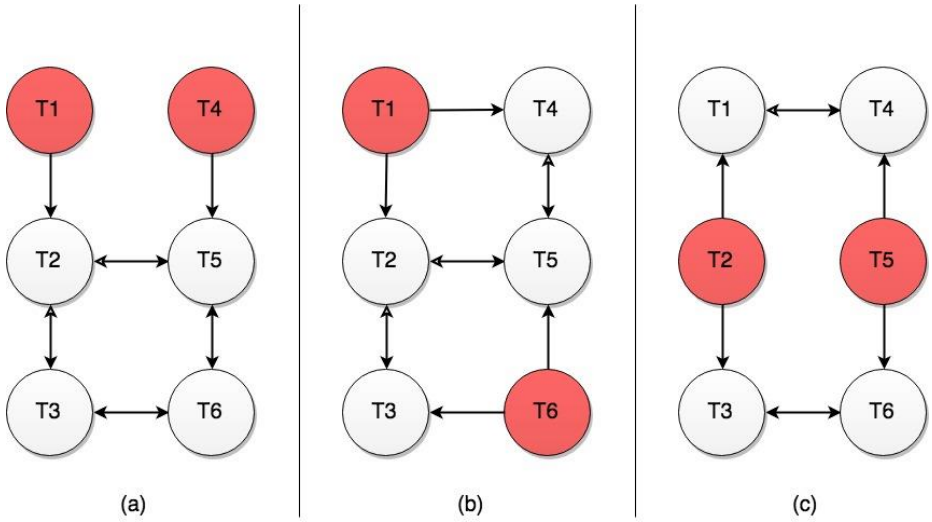


Figure 34. Examples of multiple accident scenarios in storage plant in Figure 28.

Table 25. Graph-level out-closeness for double-accidents scenarios.

Primary units	**Graph-level out-closeness**	**Risk**
T1 and T4	0.043	€ 31,099.52
T1 and T6	0.117	€ 31,101.25
T2 and T5	0.208	€ 31,198.40

Up to this point, the efficacy of vertex-level metrics and graph-level metrics in indicating criticality for cascading effects analysis have been demonstrated. With regard to cyberattack-related cascading analysis, the graph-level out-closeness analysis can be particularly useful due to the capability of cyberattacks in inflicting risk to multiple components. In the next section, how the centrality metric can be adopted for network segmentation design analysis will be described.

6.3.2 Additional Aspects of Segmentation Design

In the previous section, it has been demonstrated that the combination of accidents occurring in the most critical units in a storage plant would result in the most severe accidents than any other possible combinations. Based on this fact, it can be hypothesized that separating the units based on their criticality (i.e., vertex-level out-closeness) would lower the level of risk. Basically, separating the critical units would reduce the probability of the worst accident scenario from occurring, which will result in a more robust segmentation design.

In addition to the unit criticality, another factor that may affect the overall robustness of the segmentation design is the distribution of the tanks. To further explain this point, let us look back at the criticality analysis from Table 23. From the vertex-level out-closeness score, it has been

determined that T2 and T5 are the most critical nodes for the storage plant in Figure 28. It can be assumed that, by separating these units into different segments, a scenario in which both of these units fail at the same time can be avoided. However, this strategy alone does not effectively reduce the overall risk level of the segmentation design. For illustrative purposes, consider three segmentation designs from Table 13: NSD-22, NSD-26, and NSD-27. As illustrated in Figure 35, the most critical nodes (T2 and T5) of NSD-22 and NSD-27 are separated over the two segments. Using the previous hypothesis, that criticality-based unit distribution would result in a robust design, NSD-26 should come out as the least robust one. However, as shown in Table 26, the risk values, starting from the lowest, are NSD-22, NSD-26, and NSD-27. In this example, it is evident that separating the critical nodes alone would not be sufficient.

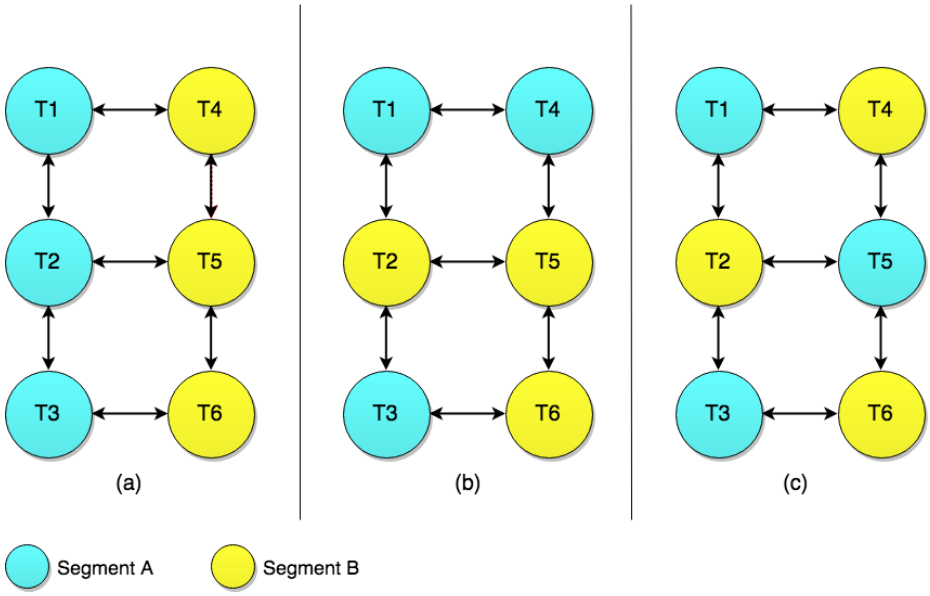


Figure 35. Directed graphs of (a) NSD-22, (b) NSD-26, and (c) NSD-27

Table 26. Risk value of graphs in Figure 35

Segmentation Design	**NSD-22**	**NSD-26**	**NSD-27**
Risk	€ 46,502.58	€ 46,657.09	€ 46,719.00

There are some other factors that partly explain why vertex-level (node-level) graph metrics cannot be solely used to identify the robustness of a segmentation design. Note that each segmentation design comprises multiple segments, and each segment represents an attack scenario. Because of that, the success of designing network segmentation depends on reducing the risk of cascading effect on every segment. Therefore, rather than focusing on reducing the risk of cascading effect for each attack scenario, a more holistic approach is needed.

For instance, the arrangement of the nodes in all segments can be presumed as one of the influencing factors of segmentation design robustness. More specifically, the design of network segmentation would influence the magnitude of escalation vectors received by every unit in the tank farm. For a better explanation, consider scenarios of attacks toward Segment A in NSD-22, NSD-26, and NSD-27. For the sake of clarity, a graph that displays the potential escalation vectors from Segment A toward Segment B is drawn in Figure 36. As depicted in Figure 36, it is apparent that, in the case of an attack in Segment A, different segmentation designs would yield different combinations of escalation vectors with varying magnitude emanated toward units in another segment. For instance,

it can be observed that, in case of accidents, the vessels within Segment B in NSD-27 (Figure 36(c)) would sustain significantly more heat radiation compared to the units of Segment B in NSD-22 (Figure 36(a)) and NSD-26 (Figure 36(b)). Evidently, NSD-27 has the highest risk level compared to NSD-22 and NSD-26. Nevertheless, the point is, in addition to the criticality at the node level, the distribution of the nodes also influences the risk of cascading effect for networks segmentation designs.

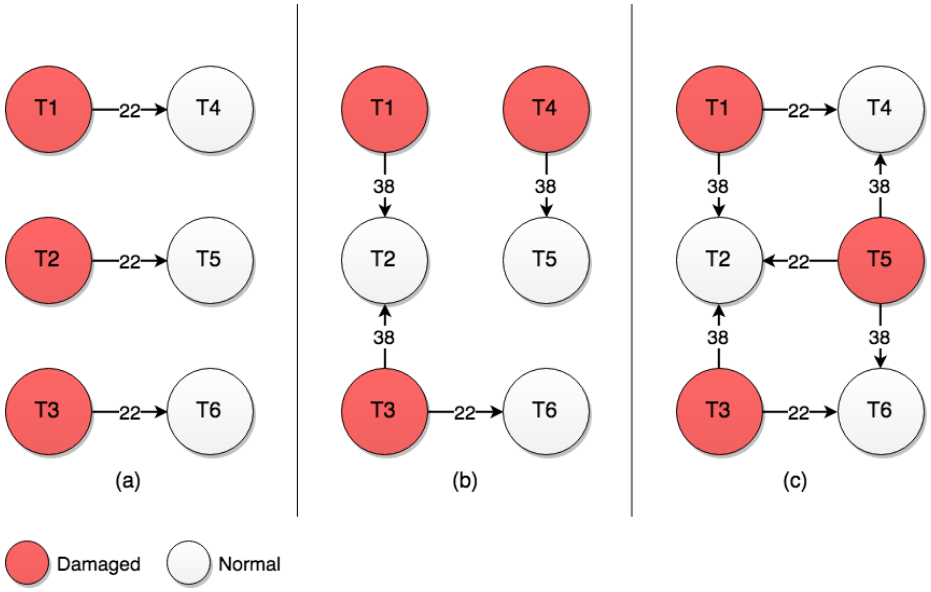


Figure 36. Escalation vectors from SgA toward SgB in (a) NSD-22, (b) NSD-26, and (c) NSD-27

Based on the analysis above, one method that can be pursued to reduce the risk of cascading effects is to segment the components based on their adjacency. If the components within the attacked segment are closely located, then most of the potential escalation vectors would be directed toward the components within the same segment instead of those in other segments. Since the components on the attacked segment are considered damaged from the attack, the potential escalation vectors directed at these components are negligible from the cascading analysis perspective.

For example, let us compare T2 in Figure 36(a) and T5 in Figure 36(c). It can be seen that both components are considered damaged and thus emitting escalation vector(s). However, due to the difference in segmentation design, the only escalation vector involving T2 in Figure 36(a) that should be considered is the vector from T2 toward T5. It should be noted that there are escalation vectors from T2 toward T1 and T3 in Figure 36(a). However, they are not drawn in the graph because T1 and T3 are considered damaged, thus the vectors would not have any effect. On the other hand, in Figure 36(c), it can be seen that T5 emits escalation vectors toward three other components from another segment, which would increase the probability of escalation. Therefore, it can be understood that the design in Figure 36(a) is more robust against the risk of cascading effects.

Up to this point, it can be presumed that grouping the adjacent components would result in a more robust design. By grouping the adjacent components, the total escalation vector directed to the other segment would be lower, thus the probability of escalation would also be lower, and eventually, the risk of cascading effects would be lower as well. On the contrary, grouping components that are distant from each other into a segment would increase the risk of cascading effects since this configuration would result in more escalation vector directed toward the other segments.

Another aspect that is crucial in mitigating cyberattack-related cascading effects is related to the initial accidents that potentially trigger the cascading effect. First, it is important to note that the risk of cyberattack-related cascading effects can be divided into two aspects: the risk of primary accidents resulting from cyberattacks and the risk of cascading effect which triggered by the primary accidents. Hence, it can be understood that to reduce the risk of cyberattack-related cascading effects, reducing the risk of primary accidents is equally crucial as reducing the risk of cascading effects.

One factor that can be analyzed to reduce the risk level of primary accidents is the equality of components distribution within the segments. In short, if the components are distributed more equally across the different network segments, the criticality of the segments would be more balanced, and the more robust the segmentation design would be. For example, see the two graphs in Figure 37. In this example, it can be seen that the two graphs have different components distribution; both segments in Figure 37(a) have three components, while Segment A and Segment B in Figure 37(b) have two and four components, respectively. Calculating the risk using the BN method, it is evident that the graph in Figure 37 (b) has a higher risk of cascading effects (see Table 27).

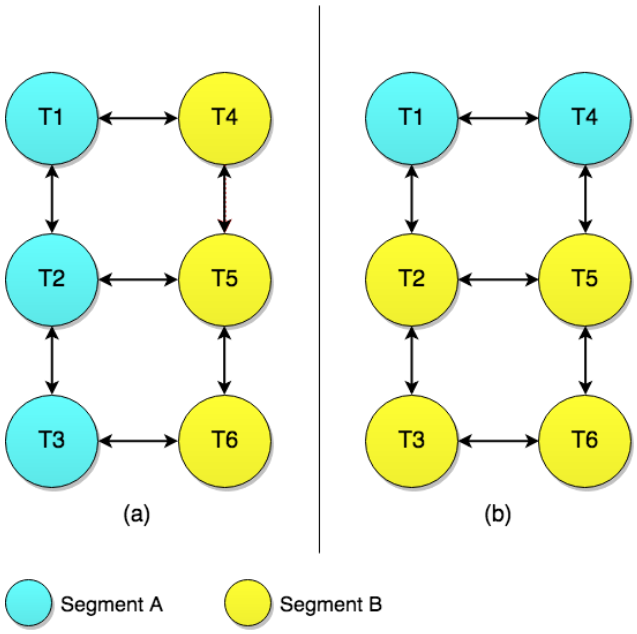


Figure 37. Directed graphs with differing segment balance

Table 27. Risks of segments from graphs in Figure 37

Design	Risk		Overall
	Segment A	Segment B	
Figure 37(a)	€ 46,502.58	€ 46,502.58	€ 46,502.58
Figure 37(b)	€ 31,099.52	€ 62,099.20	€ 62,099.20

This finding can be explained by looking at the number of components in each segment, and the game theory analysis employed in this study. In the case of Figure 37(b), unevenly distributing the components over the two segments would result in one segment with more components and one

segment with fewer components. Understandably, the segment with more components would have a higher risk relating to the primary accidents. Therefore, it can be understood that the maximum loss of the segmentation design in Figure 37(b) is higher than that of Figure 37(a). Accordingly, based on the minimax analysis, the risk of cascading effects in Figure 37(b) would also be higher.

On the other hand, equally distributing components across the two segments would result in a relatively lower risk level across the two segments, which would lead to a lower risk for the segmentation design. For instance, let us compare two design alternatives in Figure 37(a) and Figure 37(b), where the former has equal distribution, and the latter has unequal distribution. As presented in Table 27, the risk level in both segments of the graph in Figure 37(a) is roughly between both segments in Figure 37(b). Overall, the more evenly distributed components in Figure 37(a) results in lower overall risk.

To summarize the important points, there are three design strategies that need to be considered when developing network segmentation to mitigate cascading effects:

1. **Separate the critical components into different segments**. The criticality of components can be identified using the vertex-level graph metrics. Afterward, the most critical ones should be distributed into different segments.

2. **Group adjacent components into one segment**. Grouping adjacent components into the same segment would reduce the escalation vectors that are emanated toward the other segments, and accordingly would reduce the escalation probability and the risk of cascading effects.

3. **Aim for an equal number of components for every segment**. A segment with considerably more components than the others would have a higher risk of cascading effects. Because of that, this segment would become a target for adversaries, and accordingly the overall risk for the segmentation design would also be higher.

For the sake of clarity, the flowchart of processes within the risk-based methodology can be illustrated in Figure 38.

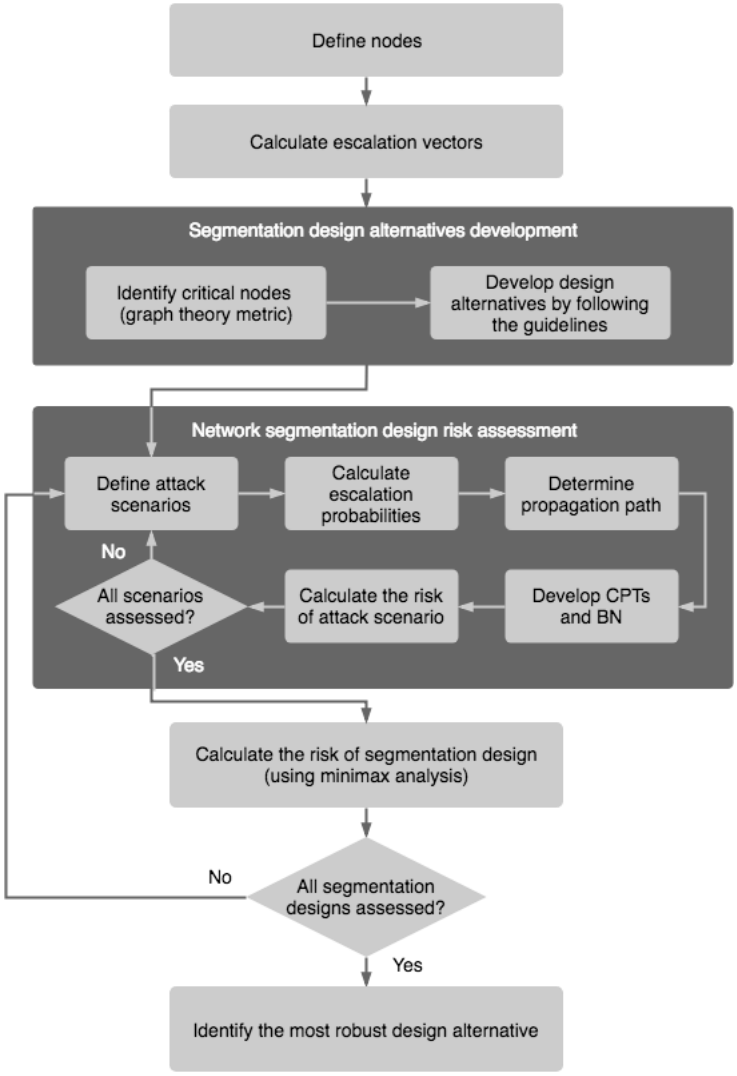


Figure 38. Flowchart of activities in the risk-based methodology developed in this study

This page intentionally left blank

7 Methodology Application: A Case Study

In the following chapter, the risk-based methodology developed in the previous chapter is demonstrated using a real case study. For this purpose, several design alternatives are considered using the guidelines developed in Subsection 6.3.2. Afterward, the risk-based methodology is applied to identify the most robust design alternative.

7.1 Case Study Description

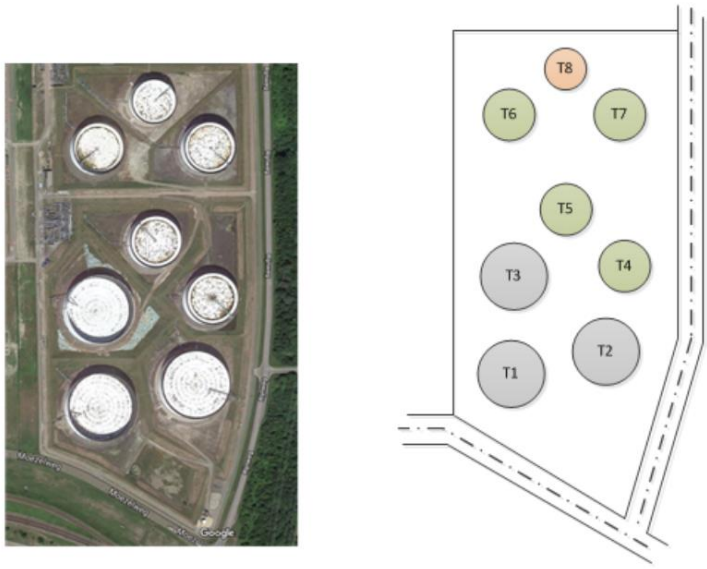


Figure 39. (a) Layout of a storage tank farm consisting of eight storage tanks. (b) Schematic of the farm with tanks IDs.

In this demonstration, a tank farm consisting of eight storage tanks of different sizes and volumes is used as a case study (Figure 39). The potential radiation intensities between the tanks are calculated using the ALOHA software, and the result is presented in Table 28. Note that only the vectors above the escalation threshold of Q_{th} = 15 kW/m^2 are presented. Moreover, for the purpose of risk assessment, the construction cost of the storage tanks are presented in Table 29.

Table 28. Heat radiation intensity (kW/m^2) Tj receives from Ti for storage plant in Figure 39

Ti↓ Tj→	T1	T2	T3	T4	T5	T6	T7	T8
T1	-	34	34	-	-	-	-	-
T2	34	-	19	34	-	-	-	-
T3	34	19	-	19	34	-	-	-
T4	-	29	15	-	30	-	-	-
T5	-	-	30	30	-	15	15	-
T6	-	-	-	-	15	-	15	32
T7	-	-	-	-	15	15	-	32
T8	-	-	-	-	-	30	30	-

Table 29. Construction cost of tanks in Figure 39 (Matches, 2014)

Tank	T1	T2	T3	T4	T5	T6	T7	T8
Vol (m^3)	39,700	39,700	39,700	25,400	25,400	25,400	25,400	17,600
Cost (Euro)	2,057,500	2,057,500	2,057,500	1,638,400	1,638,400	1,638,400	1,638,400	1,354,500

7.2 Risk-based Method Application

Based on the escalation vectors value in Table 28, a directed graph illustrating the storage tanks and the potential heat radiation intensities can be created. Using the directed graph and the heat radiation intensity table, a criticality analysis on the storage tanks can be performed. Modeling the graph using the igraph package in the RStudio software, the vertex-level out-closeness score for every storage tank can be computed. Afterward, the geometric mean of the out-closeness score and the volume for the storage tanks are calculated to indicate their criticality. The out-closeness scores and the resulting geometric mean are presented in Table 30.

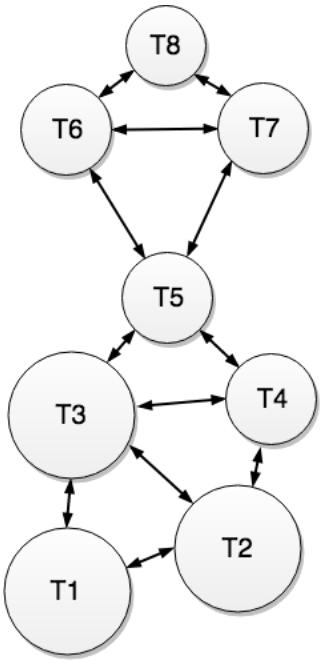


Figure 40. Illustration of potential heat radiation vectors for tank farm

Table 30. The criticality of the tanks in Figure 40

Tank	**T1**	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**
Vol (m^3)	39,700	39,700	39,700	25,400	25,400	25,400	25,400	17,600
$C_{out}(T_i)$	0.110	0.112	0.138	0.126	0.156	0.106	0.106	0.087
Cr	66.01	66.77	73.98	56.54	62.86	51.91	51.91	39.19

Note. C_{out} is the vertex-level out-closeness score, Cr is the criticality of nodes calculated using Eq. 18 in Subsection 6.3.1.

On a side note, it can be interesting to briefly discuss how the aggregation of volume affects the criticality analysis result. Using the C_{out} exclusively, the indicated critical nodes are T5, T3, and T2, descendingly. On the other hand, the Cr indicates T3, T2, and T1, as the most critical nodes, descendingly. To briefly explain the difference, let us compare how the criticality of T5 and T3 are analyzed using both methods. As indicated by their C_{out}, T3 and T5 are relatively more central than the rest of the nodes in the graph, with T5 being more central than T3. However, involving their volume into the analysis, it can be seen that the volume of T3 is larger than T5 by quite a margin. In fact, T3 is almost 50% larger in volume than T5. Due to this fact, it can be understood how the modified criticality assessment considers T3 to be more critical than T5.

7.2.1 Segmentation Design Alternatives

The next step is to develop several segmentation design alternatives for the tank farm. Previously, some guidelines for designing network segmentation have been elaborated in Subsection 6.3, via separating critical nodes, grouping adjacent nodes in one segment, and to aim for an equivalent number of components in each segment. The first guideline can be achieved by separating the critical components from being in the same segment. Based on the result in Table 30, T3, T2, and T1 can be considered as the most critical storage units descendingly. However, for this case study, seeing that the critical components are adjacent to each other, separating all of these components

would not be possible. To best satisfy the first guideline, only the top two of the critical units (i.e., T2 and T3) would be separated. The second guideline is quite straight-forward and can be applied directly during the design process. As for the third guideline, since there is an eight storage tanks and three segments, the best possible way to achieve balance is to have two segments consisting of three units and one segment consisting of two units.

For the present case, three design alternatives with an identical number of segments are developed based on the foregoing guidelines. The three designs are presented in Figure 41 as (a) NSD-1, (b) NSD-2, and (c) NSD-3. For the sake of demonstration, one additional segmentation design is developed without following any of the design guidelines, namely, NSD-4 as presented in Figure 41(d). It can be hypothesized that this design would perform worse than the other design alternatives. Now that the design alternatives have been developed, the next step is to analyze their respective risk of cascading effects to determine the most robust alternative.

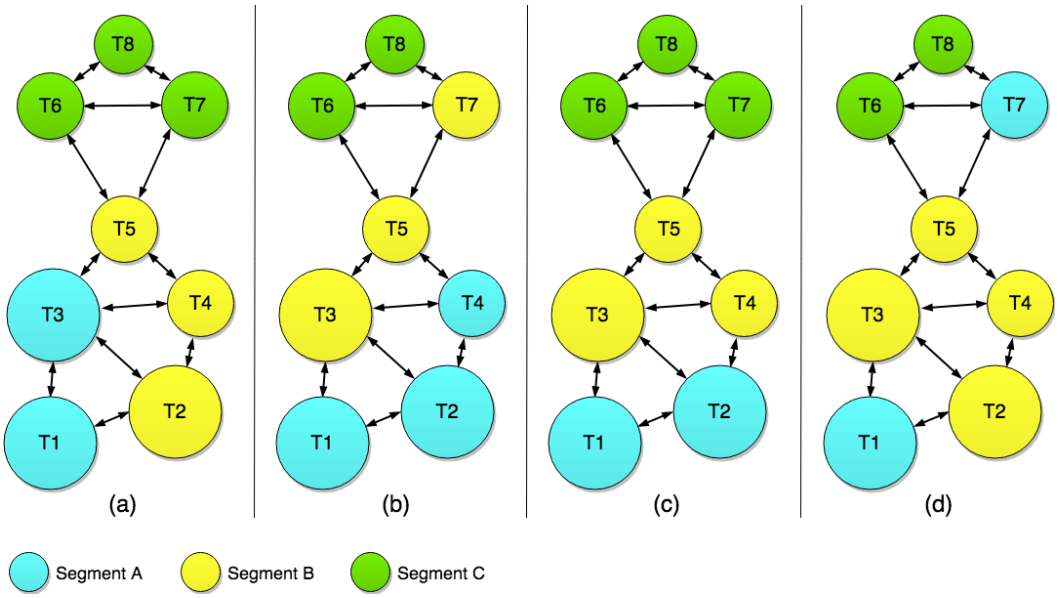


Figure 41. Illustrations of the four network segmentation design alternatives for the tank farm in Figure 39: (a) NSD-1, (b) NSD-2, (c) NSD-3, and (d) NSD-4

7.2.2 Risk Analysis

To evaluate the robustness of the designs, each design must be assessed using the developed risk-based method. Firstly, the attack scenarios for every design alternative must be defined. In this case study, there are three attack scenarios for each design alternative. For instance, Figure 42 illustrates the primary units of attack scenarios in NSD-3.

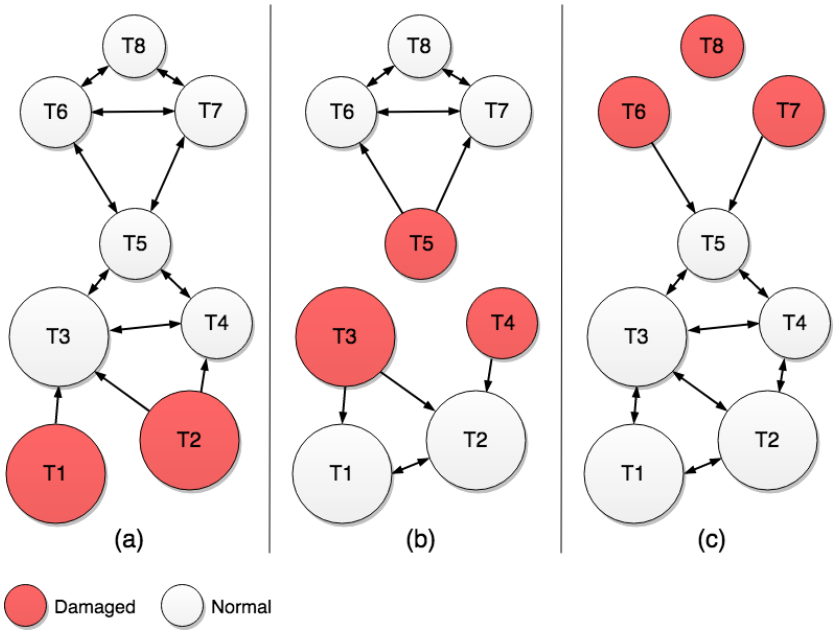


Figure 42. The graphs illustrating the primary units of the three attack scenarios in NSD-3 (see Figure 41(c))

Afterward, the BN method is applied to every attack scenario on each design alternatives to model the cascading accidents and subsequently estimate their risk. Once the risk value of all attack scenarios is obtained, the game theory analysis is utilized to derive the risk value of each segmentation design, and the result is presented in Table 31. As can be seen, NSD-3 (Figure 41(c)) has the lowest risk compared to the other alternatives and hence is the most robust design alternative. On a side note, it can also be seen that the design alternative developed without following the guidelines, i.e., NSD-4, exhibits worse robustness than the other alternatives.

Table 31. The risk of each network segmentation design in Figure 41

Design	Figure	Risk			
		Segment A	Segment B	Segment C	Overall
Non-segmented network		-	-	-	€ 68,557.00
NSD-1	Figure 41(a)	€ 21,629.31	€ 28,133.07	€ 23,158.12	€ 28,133.07
NSD-2	Figure 41(b)	€ 29,774.78	€ 27,669.39	€ 15,042.07	€ 29,774.78
NSD-3	Figure 41(c)	€ 21,627.04	€ 28,031.03	€ 23,158.12	€ 28,031.03
NSD-4	Figure 41(d)	€ 20,195.44	€ 38,647.28	€ 15,042.07	€ 38,647.28

7.2.3 Segmentation Design Implementation

Ultimately, a part of the primary objective of the present work is to develop a network segmentation. One example of network segmentation implementation based on the design developed in the previous section is illustrated in Figure 43. However, it cannot be emphasized enough that this implementation is just one possible way to implement the design as there can be myriad of other factors that might influence the final design of network segmentation. Nevertheless, as long as the

segmentation design from the risk-based methodology is taken into account for the network design, the security benefit against cyberattack-related cascading effects can be attained.

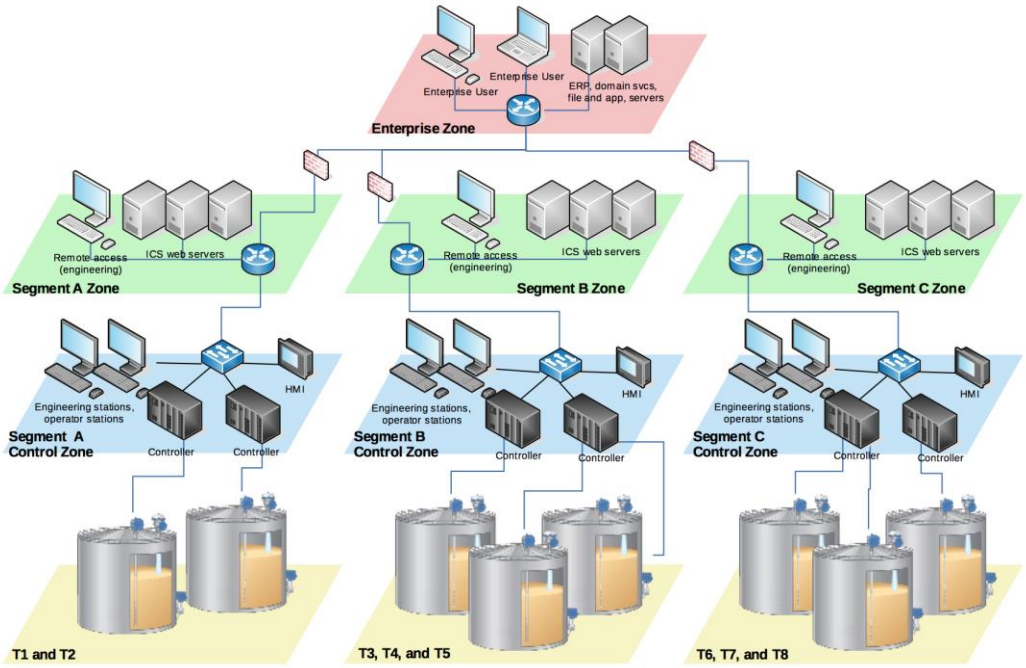


Figure 43. Example of network design based on NSD-3 (Figure 41(c))

8 Discussions

In this chapter, some of the key findings from the previous chapter are further discussed. The goal of this chapter is to explain the significance of the results from several perspectives further. In Subsection 8.1, the proposed risk mitigation technique is discussed from the standpoint of cyber risk management. In Subsection 8.2, a discussion from the perspective of security investment and management is also presented to gain insight about the optimality of investing in the proposed risk mitigation technique. Lastly, Subsection 8.3 concludes the critical points from the discussions.

8.1 Cyber Risk Management Perspective

The main accomplishments of this thesis are twofold: (1) a risk evaluation method for cyberattack-related cascading effects based on BN method, and (2) a demonstration of network segmentation as an effective means to mitigate the risk of cyberattack-related cascading effects. However, in practice, the existence of risk does not in itself warrant a risk mitigation effort. This can be understood by looking from the perspective of cyber risk management. Referring to cyber risk management, the two main contributions mentioned above can also be seen as part of the risk assessment cycle: the BN method is part of risk evaluation, while the proposed solution can be considered as part of risk mitigation or risk reduction strategy. Between the risk evaluation and implementing risk mitigation strategy, generally, risk assessment also includes an activity in which potential risk management strategies are developed and evaluated in order to determine the most optimal option. Therefore, it can be comprehended that some analyses are undertaken before deciding on the risk mitigation strategy.

To be more precise, let us loosely refer to some formal definitions. For instance, from the NIST risk assessment methodology (see Appendix), it can be understood that the application of the BN method for risk assessment correspond to several steps in the NIST risk assessment methodology, namely “likelihood determination”, “impact analysis”, and “risk determination” (Stoneburner et al., 2002). On the other hand, the risk mitigation technique proposed in this thesis can be seen as an outcome of “control recommendation” activity. In risk determination and control recommendation activities, there are activities that are described as “to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization’s operations.” Moreover, Stoneburner et al. (2002) also mention some factors to consider when developing the risk mitigation options, namely the efficacy of the options, governmental regulation, internal organizational policy, impacts to daily operations, etc. Depending on these factors, the strategy to deal with similar risks could be different from one organization to another.

As can be understood, the activity mentioned above is critical to risk management process. To sum up, the point of discussion is having proved that network segmentation can be an effective control measure to mitigate the risk of cyberattack-related cascading effects does not imply that this strategy should be pursued as there can be a more optimal risk mitigation strategy. On that premise, some brief analyses of the possible risk management strategies to deal with cyberattack-related cascading

effects, while considering some relevant factors, are presented in this subsection. The goal is to gain some insight on the optimality of the risk mitigation technique proposed in this thesis compared to the alternative strategies.

The first possible risk management strategy is risk acceptance. First and foremost, before considering this strategy, organizations must refer to the applicable regulations. If there is any regulation which obliges system owners to control or mitigate a particular risk, then the risk acceptance strategy should not be undertaken regardless of the outcome of risk assessment. By the time this thesis is written, there is no regulation specifically related to cyberattack-related cascading effects. One regulation that specifically mentions cascading (domino) effects is the European "Seveso" directive, albeit it does not mandate the undertaking of security analyses nor the implementation of additional security measures (G. L. Reniers & Audenaert, 2014). However, it is understood that most organizations would consider accepting the risk of cyberattack-related cascading effects, or cascading effects in general, primarily because they consider the probability occurrence of such accident being too low (G. Reniers & Cozzani, 2013). Indeed, most organizations barely take into account high-impact, low-probability (HILP) events in their risk assessment and management plan (Khakzad et al., 2018). Nonetheless, the decision about whether to accept such risk should refer to the risk acceptance level of each organization: if the identified risk is well below the risk acceptance threshold of the organization, then the risk can be accepted, and no particular actions must be undertaken. Conversely, in cases where the level of risk is higher than the acceptable level, then other risk strategies should be considered.

The next risk management strategy is risk reduction. To the best of our knowledge, the solution proposed in this thesis is the first attempt to mitigate the risk of cyberattack-related cascading effects. Because there are no other options to be compared, the proposed solution will be compared to other risk strategies. Another possible risk management strategy is risk transfer. In practice, this is most likely to be done by taking cyber insurance. However, cyber insurance products relating to ICS is still rare although the consequences of cyberattacks toward ICSs can be much more severe than, for instance, the case of data loss (Kozak et al., 2016). Several reasons hamper the growth of the cyber insurance industry, but that is out of the scope of this discussion.

Lastly, another possible risk mitigation strategy is risk avoidance. In practice, risk avoidance strategy for cyberattack-related cascading effects can be accomplished, for example, by removing Internet connectivity from ICS components. Lennon (2013) suggested that an indication of ICS being targeted of cyberattacks should be enough to get system owners to disconnect ICS components from the Internet. However, even though it looks like a viable strategy, it can be expected that this strategy would adversely affect the productivity and efficiency of the facility. Therefore, the drawbacks that come with the strategy must be carefully calculated and weighed against the expected security benefits before such a strategy can be taken. Without overlooking the importance of a proper cost-benefit analysis, it is conjectured that the drawbacks from removing Internet connectivity from ICS components would outweigh the yielded security benefit.

8.2 Security Investment and Management Perspective

In addition to the cyber risk management perspective, discussing the findings from the perspective of the economics of cybersecurity can also be interesting. Evaluating the findings from this perspective would allow us to evaluate whether investing in such security measure is optimal from the perspective of security investment. Moreover, for the cyber risk managers, the goal is to be able to frame and present the cost of security investment (i.e., direct and indirect costs) and the potential security benefits in a universal language that can be understood by executives and senior management alike. Hence, this type of analysis is not only beneficial to investigate the security investment options, but also to facilitate communication with the other stakeholders.

There are several analyses that can be done. For instance, ROSI (Return on Security Investment) analysis allows the comparison between different security investment options. Considering the present work is the only option in mitigating the risk of cyberattack-related cascading effects, a ROSI analysis would not provide much insight.

Another type of analysis which can be performed is a cost-benefit analysis. One interesting point of discussion regarding network segmentation is how its application might entail some drawbacks that can be regarded as added costs. As elaborated in Subsection 5.3, the adoption of network segmentation also carries some potential drawbacks, such as extra maintenance cost, loss of productivity, etc. From the perspective of businesses and organizations, these drawbacks can be considered as added costs. Without understanding the significance of these added costs, it can be difficult to conclude whether the adoption of network segmentation would be beneficial. If the added costs are higher than the security benefit, then it can be difficult to justify the adoption of this control measure. Therefore, it can be essential to understanding the significance of the added costs.

For illustration purpose, let us do some analyses on the security benefits and the potential added costs of the case study presented in Chapter 7. Accordingly, both the security benefit and the potential added cost must first be calculated. Firstly, the benefit aspect can be defined as the reduced risk resulting from the implementation of network segmentation. More specifically, the benefit can be measured as the difference of risk between the segmented network and the non-segmented network. The risk analysis on the case study has been done in Chapter 7. Subtracting the risk level of the segmented network from the risk level of the non-segmented network (see Table 31), the reduced risk is estimated at € 68,557.00 - € 28,031.03 = € 40,525.97.

Next, the cost aspect can be defined as the increase of maintenance and operation costs due to the utilization of network segmentation. As previously mentioned in Subsection 5.3, several elements contribute to the added costs. However, for the sake of simplicity, only the increase in maintenance cost is taken into consideration. To estimate the increase in maintenance costs, the Eq. 11 introduced in Subsection 5.3.2 can be utilized. To start with the calculation, the maintenance cost for the non-segmented network MC_n is assumed at $ 30,000.00 per year, or approximately € 25,000.00 per year (Honeywell, 2011). Next, the $C(env, nsd)$ score for the non-segmented and the segmented network is calculated using Eq. 9 and the results are (env, nsd_n) = 2.52 E-03 for the non-segmented and (env, nsd_s) = 3.63 E-03 for the segmented network. Next, the scale factor is obtained by dividing $C(env, nsd_s)$ by $C(env, nsd_n)$, and the result is z = 3.63 E-03/2.52 E-03 = 1.44. Lastly, by multiplying the scale factor with the basic maintenance cost, the increased maintenance cost is estimated at $MC_s = z \times MC_n$ = 1.44 × € 25,000.00 = € 36,000.00. Therefore, the amount of the added costs is approximated at € 36,000.00 - € 25,000.00 = € 11,000.00.

Now that the benefits of security and the increased maintenance cost have been calculated, some analyses can be undertaken. Firstly, it is easy to be enticed into directly juxtapose the reduced risk with the increased maintenance cost. However, it is important to note that maintenance cost is a recurring expense. Hence, if the implementation of network segmentation causes the maintenance costs to increase, the added costs would be recurring as well. On the other hand, the security benefit is attained when an attack happens. Clearly, it can be understood that these aspects cannot be directly compared. One approach that can be taken is to calculate the number of years before the accrued added costs exceed the security benefits. Assuming that it would take t years for the accrued added cost to exceed the security benefits, then the security investment would yield benefits for the organization if it can be expected that cyberattack towards ICSs would be occurring at least once in t years.

Following the aforementioned approach, the security benefits can be divided by the annual added costs, and it can be estimated that the total expense for the increased maintenance cost would surpass the security benefits in € 40,525.97/€ 11,000.00 = 3.68 years. Therefore, for the case study in Chapter 7, the investment decision would be considered optimal if a cyberattack towards ICSs would be attempted against the facility at least once in every 3.68 years. It is important to note that

this finding is produced with an underlying assumption that the chosen number of segments is the most optimal. It is understood that the different number of segments would yield different security benefits as well as a different increase in IT maintenance costs. Therefore, this finding is only applicable to that specific network segmentation design with a particular number of segments, and different network segmentation design would be likely to yield a different conclusion.

8.3 Conclusion

Now that all possible risk management strategies have been discussed, some insights regarding the significance of the risk reduction solution presented in this study can be derived. Firstly, from the brief analyses, risk avoidance and risk transfer can be regarded as less optimal strategies. Risk avoidance can be deemed unlikely due to the trade-offs that must be sustained by the organization. Unless a comprehensive analysis of the trade-offs can indicate a positive outcome for the company, which is unlikely, then this strategy would be likely to yield negative trade-offs. Taking a risk transfer strategy is also seems unlikely due to the underdeveloped ICS cyber insurance market, although the increasing trend of cyberattacks against ICS might change this situation in the near future.

Risk acceptance is most likely the strategy that would be opted by businesses and organization in dealing with the risk cyberattack-related cascading effects, as most organizations would not take HILP events into account. Hence, looking at the current trend, it looks unlikely for organizations to immediately adopt network segmentation to reduce the risk of cyberattack-related cascading effects given that they have already overlooked the other HILP events. Moreover, the presence of added costs from the implementation of this solution potentially reduce the appeal of this solution. Unless there is a substantial change that force organizations to mitigate cyberattack-related cascading effects, such as the development of new regulations, it is difficult to see how the solution presented in this thesis would significantly change how organizations manage this type of risk. Nevertheless, if an organization consider the risk as higher than the acceptable level, the risk reduction technique can readily be adopted to bring the risk level down to an acceptable level.

Moreover, another point of view is to take a more holistic view of the implementation of ICS network segmentation. Network segmentation is essentially a system architectural change which would affect various aspects of the system and the organizations; its implementation may yield some benefits and drawbacks. Indeed, there are still debates on whether the benefits of network segmentation implementation would outweigh its drawbacks. It can be presumed that the extent of benefits and drawbacks would be different in different organizations. Hence, a careful assessment of the factors affected by the implementation of network segmentation would be essential to fully understand whether its utilization would yield a positive outcome for an organization.

With regard to the debates mentioned above, the finding of this thesis may contribute to the list of benefits that can be gained from the adoption of network segmentation. As shown in Table 31, the implementation of network segmentation, even when the design is not optimized to mitigate the risk of cyberattack-related cascading effects, would still yield a cascading risk reduction benefit for the facility (albeit not as optimal). Thus, if network segmentation is implemented in a facility regardless of its objective, it can be expected that the risk of cyberattack-related cascading effects in the facility would be reduced nonetheless. In that sense, the finding of this thesis presents another positive factor when considering the implementation of network segmentation.

9 Conclusions

This chapter discusses and summarizes the key findings in this study. The first part of this chapter provides the conclusions of this research. Firstly, the formulated research questions of this study are revisited, and the answers to the research questions are summarized to show if and how the research objectives have been achieved. Afterward, the contributions, some limitations of the research, and a reflection on the execution of the research are elaborated. Finally, some recommendations for future research are offered.

9.1 Research Questions Revisited

The adoption of ICSs in chemical and process plants has enabled cyberattacks to cause physical damages to these facilities. Considering the vulnerability of ICSs and the risk of triggering cascading effects, a mitigation strategy is pursued in the present study. Therefore, the primary objective of this study is to improve the robustness of the chemical plants against the risk of cyberattack-related cascading effects by utilizing network segmentation. From this research objective, the main research question was developed:

> **Main Research Question** – How to optimize ICS network segmentation design in chemical plants to improve its robustness against cascading effects under cyberattacks?

Further, the main research question was broken down into a series of sub-research questions to guide the process of answering the main research question, and subsequently fulfilling the research objective. Based on the findings of this study, the answer to the sub-research questions can be presented as follow:

> **Sub-research Question 1** – How do cyberattack-related cascading effects happen in chemical and process plants?

Despite the apparent potential of cyberattacks to trigger cascading effects in chemical and process plants as mentioned in several reports and academic journals, there has been no record of cyberattack-related cascading incidents. Since it is not possible to learn about cyberattack-related cascading effects from past incidents, an alternative approach of deep-dive analysis to the relevant domains of knowledge was pursued. Cyberattack-related cascading effects would involve at least three domains of knowledge, namely cascading effects, ICSs (Industrial Control Systems), and cybersecurity. Therefore, by understanding the related domains in the context of chemical and process plants, how cyberattack-related cascading effects can potentially occur was investigated.

Firstly, an exploration to the ICS literatures in the context of chemical and process plant was conducted. It was learned that there are various types of ICS components, namely pumps, valves, and gauges. These components are critical to the operations in chemical and process plants, and thus their misuse would potentially lead to disastrous consequences. Subsequently, the

cybersecurity aspect of ICS was investigated. One critical aspect regarding the cybersecurity of ICSs is their vulnerability against cyberattacks. In fact, there have already been some reports on cyberattacks toward ICSs in various industrial facilities.

Once the possibility of cyberattacks against ICS was established, the last step was to investigate the potential impact of cyberattacks on ICS. Some literature has explored the possible outcomes of ICS cyberattacks, including the disruption of operations and damage to equipment. Some of the potential impacts have been regarded as potential triggers for cascading effects. For instance, cyberattacks on ICS can possibly result in a major release of hazardous chemicals, which could lead to vapor cloud explosions (VCE) or pool fires (PFs). Both of these accidents have been recognized as possible triggering events for cascading effects.

To conclude, cyberattacks on ICS components have not only been demonstrated in an experimental setup but also have been witnessed to occur in real-world situations. This type of cyberattacks might lead to various consequences, which in the worst-case scenario, can lead to cascading accidents.

Sub-research Question 2 – How to model and analyze cyberattack-related cascading effects using Bayesian network?

A Bayesian network (BN) based method to model and analyze cascading effects has been developed in a previous study (Khakzad et al., 2013). To utilize the BN method for the present study, in-depth analyses were conducted on cyberattacks toward chemical plants and the influence of network design on cyberattacks. The inclusion of network design into the model was particularly critical due to the need of evaluating the impact of network segmentation design on the risk of cyberattack-related cascading effects. Moreover, to integrate the BN method, the cyberattack analysis, and the network design, several important assumptions were made: (1) network segmentation would contain the consequence of cyberattacks within the breached segment, (2) the goal of the adversaries is to inflict maximum damage, and (3) the adversaries only have enough resource to attack one segment. The implication of the assumptions in the implementation of network segmentation would force the adversaries to choose a single segment that yields the most damage.

Taking the findings from the analyses and the assumptions into account, a methodology to model and analyze cyberattack-related cascading effects in a particular network segmentation design was developed, the process flow of which can be described as follow:

1. Firstly, based on the segmentation design, the process units in the plant can be grouped according to the segmentation. For each segment, an attack scenario can be defined in which the units within the segment are considered as the primary accidents.
2. Next, using the BN method, the probability of damage for each unit for every attack scenario can be determined. Accordingly, the risk of cascading effects can be calculated.
3. After the risk of each attack scenario has been calculated, the risk scores are consolidated into a single value using minimax analysis from game theory. The consolidated risk score would represent the robustness of the network segmentation design against cyberattack-related cascading effects.

Sub-research Question 3 – What are the factors of ICS network segmentation design that can influence cascading effects in chemical plants? How can these factors contribute to mitigate cascading effects in case of cyberattack?

From the analysis of network segmentation and cascading effects, there are three factors of network segmentation design that influence the risk of cyberattack-related cascading effects. The first factor is the distribution of critical process units. The criticality of process units in process plants with regard to cascading effects has been explored in the previous studies (Khakzad & Reniers, 2015). Briefly, accidents occurring in the critical units would potentially lead to more severe cascading

effects. In mitigating cyberattack-related cascading effects, separating the critical units into different segments was found to reduce the risk of cascading effects.

The second factor is the number of process units in each segment. This study found that segmentation designs in which the units are equally distributed tend to have higher robustness against the risk of cascading effects. Conversely, designs in which some of the segments contain significantly more units than the others are likely to be less robust. The third factor is the distribution pattern of the process units within the segments. Furthermore, it was found that the designs where the adjacent process units are grouped within the same segment would result in a lower risk of cascading effects. On the other hand, the designs where distant units are grouped within the same segments tend to have lower robustness.

> **Sub-research Question 4** – To what extent does the segmentation design modification mitigate the risk of cyberattack-related cascading effects?

The efficacy of the developed methodology in mitigating cyberattack-related cascading effects can be evaluated by comparing the risk scores among the designs. In the Methodology Application in Chapter 7, one design was developed by following the design guidelines, and another design was developed without following any of the guidelines. Also, the risk of the non-segmented system based on the same case study was presented. As presented in Table 32, implementing network segmentation even without following any of the design guidelines shows a significant risk reduction of about 45%. Moreover, by using the guidelines to develop the network segmentation, approximately a further 25% risk reduction can be achieved. Finally, comparing the segmentation design based on the guidelines with a case where no segmentation was performed showed a reduction of 55% in the risk of cascading effect.

Table 32. Risks level of different network designs for the case study in Figure 39

Segmentation Design	Risk of Cascading Effects
Segmented network (with guidelines)	€ 28,031.03
Segmented network (without guidelines)	€ 38,647.28
Non-segmented (flat) network	€ 68,557.00

9.2 Contributions

9.2.1 Academic Contributions

From the scientific perspective, this study attempts to fill the knowledge gap of cyberattacks and cascading effects in chemical plants. The contribution of this research, which is to develop a cascading effects mitigation methodology from cyberattacks in chemical plants, is the first attempt to mitigate cyberattack-related cascading effects in chemical plants. To the best of our knowledge, this study is also one of the earliest works that study the relationship between cascading effects and cyberattacks. Also, this study can be a stepping stone for future studies on mitigating cyberattack-related cascading effects, either in chemical plants or other domains.

Moreover, the main contributions of the present work is threefold: (1) developed a risk evaluation method for cyberattack-related cascading effects using the BN method, (2) demonstrated the efficacy of network segmentation in mitigating the risk of cyberattack-related cascading effects, and (3) identified the critical design aspects of network segmentation that contribute to the

robustness of the designs. It needs to be acknowledged that some parts the present study are developed based on prior works. For example, by using the BN method developed by Khakzad et al. (2013) as a basis, this thesis extends the method to model the impact and estimate the risk of cyberattack-related cascading effects while taking into account the implication of network segmentation. Moreover, this study also uses the graph-theoretic approach as introduced by Khakzad and Reniers (2015) as a starting point to identify the crucial design aspects of network segmentation. Based on these aspects, a set of design guidelines for network segmentation was developed to help improve the robustness of systems against cyberattack-related cascading effects.

Furthermore, another contribution of the present work is that it presents a method to quantify one benefit aspect of network segmentation. As previously mentioned, network segmentation is a fundamental modification to the network architecture that may yield multifaceted effects to systems and organizations. It can be essential to estimate the benefits and drawbacks of its implementation to gain a more comprehensive understanding regarding the trade-offs.

9.2.2 Practical Recommendation

From a practical perspective, there are several main recommendations that can be derived from this thesis. First, the present study has shown ICS network segmentation as an effective control measure against the risk of cyberattack-related cascading effects. It has been shown that risk acceptance might still be the most optimal risk management strategy for cyberattack-related cascading effects risk. However, cyberattacks toward ICS in industrial facilities have been showing an increasing trend and predicted to continue to increase in the future. Moreover, the present study also offers a risk-based methodology and design guidelines for designing robust network segmentation. If an organization decides to implement network segmentation to mitigate cyberattack-related cascading effects, the risk-based methodology can be readily used. Moreover, a set of design guidelines for network segmentation can also be utilized by network designers to develop network segmentation design alternatives that would exhibit robustness against cyberattack-related cascading effects. By developing these two approaches, businesses and organizations are presented with an effective risk reduction option to mitigate cyberattack-related cascading effects. If such a situation occurs become cyberattacks toward ICSs become much more frequent, having a risk mitigation strategy can be crucial to the security of these facilities.

Secondly, the findings of this study potentially add a supporting factor for organizations to adopt network segmentation. During the methodology application, it has been found that the implementation of network segmentation would reduce the risk of cyberattack-related cascading effects even in the case where the network segmentation design is not optimized for mitigating cyberattack-related cascading effects risk. This finding may contribute to the debate on the trade-offs associated with the implementation of network segmentation by providing a quantitative analysis of the benefit of this control measure.

9.3 Research Limitations

During the development of the methodology, there were some limitations that hampered the progress of the work, and there are some others that need to be outlined so the outcome of the study can be interpreted accordingly. These limitations affect different parts of this study, and some of them have been described in their respective sections. In this section, the limitations are summarized and elaborated further.

9.3.1 Accuracy of the Building Blocks

The risk-based methodology developed in this study is built upon several building blocks, such as the BN method (Khakzad et al., 2013), the probit method (Cozzani et al., 2005), the minimax analysis from game theory (Cox, 2009), and others. For some of these methods, there are more

sophisticated methods available. For instance, Khakzad (2015) proposed a method based on dynamic Bayesian network (DBN) capable of modeling both the spatial and temporal aspects of cascading effects. Clearly, DBN would offer a more accurate likelihood estimation, and accordingly, a more reliable risk assessment result.

Hence, it can be inferred that the inherent limitation of conventional BN in modeling cascading effects would impact the overall accuracy of the methodology. Consequently, since the design guidelines are developed based on the application of methodology, the efficacy of the design guidelines for the network segmentation also largely depends on the accuracy of the methods.

9.3.2 Associating ICS Components and Potential Accidents

The issue of associating cyberattacks with potential accidents has been described at length in Subsection 5.2.3.1 and 5.2.3.2. To recap the issue briefly, even though both the cyberattacks-related physical accidents through ICSs have been reported in real life and their possibility has been demonstrated in an experiment, their exact mechanism can be challenging to understand. Several factors contribute to this issue, such as the complexity of chemical plants and how chemical plants can be different from one another.

To deal with this issue, the product-flow based approach (see Subsection 5.2.3.2) has been employed. However, as previously explained, there are drawbacks to this approach, including the simplifying assumption made for associating ICS components to the potential accidents of the process units. As the more accurate report-based approach would be difficult to pursue, this study settles with a simpler approach.

9.3.3 Limitations of Game Theory

The risk-based methodology developed in this work employs game theory to consolidate the possibility of cyberattacks and risk analysis in the network segmentation. However, it must be noted that there are underlying assumptions in the game theory. The assumptions primarily concern the nature of the adversaries, e.g., the attackers are rational, possess all the required information for making decisions, and are capable of analyzing the potential outcome of all possible strategies. Due to its implausibility, these assumptions often become the point of critics.

9.4 Recommendations for Future Research

The limitations affecting this research have to a certain extent held back the process of the study and accordingly its outcomes. Based on these limitations, some directions for future research and improvement are presented here:

1. **Adopt more sophisticated methods for the methodology**. The risk-based methodology can be further improved by replacing the currently used BN method with DBN method. Moreover, it would be intriguing to see whether the outcome of the study would change when different methods are used.

2. **The relationship between ICS components and potential accidents.** A study of cyberattacks to ICSs in chemical and process plants and their potential outcome could be another point worth of studying. With regard to the present study, understanding the potential implication of cyberattacks to ICS in chemical plants would help associate ICS components to the potential accidents. More generally, the outcome of this research might be used to help design a safer and more robust network design in chemical plants.

3. **Alternative to game theory**. The game theory approach used in this study presents several limitations from the underlying assumptions used. Another approach, such as the

utilization of agent-based modeling (ABM) to simulate the adversaries, can be explored as an alternative to game theory.

In addition to the recommendations based on the research limitations, other ideas that might improve the outcome of this study could be:

1. **A method for determining the optimal number of segments.** In the present study, the number of segments was assumed as an outcome of a pre-analysis. The problem is there is not yet a method to determine the optimal number of segments. However, in Subsection 0, a cost-benefit analysis has been conducted to evaluate the benefits of implementing network segmentation against its drawbacks. Following a similar approach, a framework to evaluate the optimal number of segments can be developed.

2. **To expand the risk calculation**. In the present study, the damage was defined as the physical damage to the process units. From the land-use planning perspective, this risk is referred to as on-site risk. In addition to this, another category of risk exists, namely the off-site risk. Off-site risks, or external risks, account the risks imposed to points of interest outside the plants, such as nearby residential communities. The inclusion of off-site risk into the risk-based methodology could be an interesting direction for future research.

3. **Taking safety measures into account**. Chemical and process plants implement various kinds of safety measures (i.e., add-on safety barriers), such as water deluge systems (WDS) or fireproof coating (FPC). The implementation of safety barriers would eventually affect the propagation of accidents, and therefore, the risk of cascading effects. It would be interesting to see whether the application of physical protection mechanisms would affect the outcomes and recommendations made in the present study.

4. **A more holistic analysis of the benefits and impacts of network segmentation**. The implementation of network segmentation would eventually bring various benefits, such as cybersecurity improvement, increase of system performance and reliability, and the mitigation of cascading risk-benefit. On the other hand, a number of drawbacks would also be sustained, such as the increased maintenance and operational cost or reduced productivity. Currently, most of analyses only investigate network segmentation from a single perspective. An analysis that takes all these factors into account could provide a comprehensive view of the benefits (and the drawbacks) of using network segmentation.

9.5 Reflections on Research Process

In this section, we have presented reflective thinking about the execution of this work. This section provides an opportunity for us to reflect upon the process we have followed, the decisions that have been made, and ultimately what we have learned from this process. Lastly, we will provide some retrospective remarks about how this master's thesis fulfills the requirement of Management of Technology (MoT) programme.

The breadth of background knowledge needed for this master's thesis presents plenty of challenges during the execution of this thesis. To our understanding, the theme of this thesis at least involves three different research themes, namely cascading effect, cybersecurity, and industrial control systems (ICS), all within the context of chemical and process plants.

Hence, it can be seen that we had much ground to cover before we can fulfill the research objectives of this master's thesis. To compensate for the lack of background knowledge, we did an extensive literature review to gain a basic understanding of the remaining relevant domains of knowledge. As a result, our preliminary literature review comprised more than 30 pages and 15 subsections

covering the essentials of the relevant domains, not to mention that this was after subtracting some parts that are considered less relevant.

There were a couple of challenges that arose from this issue. One of the impacts from the breadth of the background knowledge was our unfamiliarity with some of the relevant keywords. For example, the term "network segmentation" was not discovered until roughly four months into the thesis writing process. Prior to that, we were using the term “system layout design” to represent network design, and also “ICS system layout modification” to represent network segmentation. This example shows that to achieve the primary objective of this master’s thesis, a broad, albeit not deep, comprehension of the relevant domains involved is required. On a side note, it seemed to us that a large amount of literature reviews on this type of study was inevitable.

Moreover, despite the multi-domain nature of the research topic, the cyber risk management point-of-view taken in this work has been certain from the start. In other words, the intended audience of this work is people from the cyber risk management background. However, keeping the perspective consistent throughout the execution of this thesis was surprisingly challenging. For instance, during the literature review, there was a consideration about which details should be presented. Referring to the pre-determined perspective, deep dive analyses into cascading effects and network segmentation in ICS would be appropriate. However, a section describing the basic of cyber risk management may not be as useful. Indeed, during the early literature review, we initially presented some basic knowledge regarding cybersecurity management, such as the CIA triad[12] concept. However, looking back to our intended readers, this section was deemed unnecessary and was subsequently removed. The important thing learned was regularly reminding yourself of the intended audience of this study has been a useful way to determine which discussions are relevant to this study, thus the perspective of this study can be maintained.

There was another challenge in balancing the need to reduce uncertainty and maintaining the scope of the discussion. It has been mentioned that network segmentation in ICS is a common cybersecurity control measure, and the novel aspect of the solution proposed in this work is its utilization for mitigating cyberattack-related cascading effects. Therefore, even though there is no need to prove the feasibility of network segmentation as a control measure (because it is already a common practice), a feasibility study regarding the specific utilization as proposed in this work is still required. Our initial approach to the feasibility study is to review literature and reports looking for similar real-world implementation. If a similar example can be found, then the feasibility of the solution can be confirmed. However, as will be explained in the next paragraph, examples of ICS network designs can be very difficult to find. Another approach is to meticulously inspect the technical and operational feasibility of the proposed design in the chemical plant's settings. The downside of taking this approach is we are risking to stretch the scope of this work into the technical realm of chemical plants and its operation. Ultimately, interviews with practitioners were conducted to investigate the feasibility of the solution, during which the feasibility was confirmed. By relying on experts’ opinion, we have managed to conclude the feasibility study while maintaining the scope of the work.

Furthermore, we have experienced some challenges caused by the unavailability of real-world ICS network design in chemical plants. Having a real-world example would considerably assist our work, such as by confirming the possibility of the solution without involving too many assumptions. However, being a security sensitive information, it can be understood that this information would not be easily attainable by searching through the Internet. Although the reason seems obvious at this point, it was not the case during the early execution of this thesis. Consequently, a considerable amount of time was spent searching for an example of an ICS network design. As previously mentioned, this issue was finally resolved after the interviews with experts. One of the practitioners

[12] CIA triad refers to the three security objectives (or attributes) for information and information systems, namely confidentiality, integrity, and availability.

we interviewed the difficulty of finding a real-world example and suggested to use one of the reference architectures from the available reports and whitepapers.

Another interesting point of reflection is how we coped with the lack of earlier studies on how cyberattacks lead to physical accidents in the context of chemical plants. To explain it again briefly, the relationship between cyberattacks on ICS and the potential accidents was found to be less studied. Without a framework or model to explain this relationship, it was not possible to determine which process units would be damaged by the misuse of which ICS components. This is particularly important to the present study because the analysis of cascading effects would have to be "translated" into the ICS network segmentation design. In the present work, we adopted a simplifying assumption that associate the ICS components to the nearest process units based on the chemical product flow. We did identify another possible approach based on accidents report. However, the product flow approach was deemed to be the more feasible approach between the two. Nevertheless, seeing the importance of this type of study, we would be eager to see more research toward this direction in the near future.

Relevance to the Management of Technology (MoT) Study Programme

Lastly, we will reflect on how this master's thesis exhibit the fulfillment of the graduation criteria of the Management of Technology study programme. The first criterion requires the study to focus on problems within a technological context. The primary objective of this study is to achieve an improvement in the system's robustness against the risk of cyberattack-related cascading effects, which has been achieved through the utilization of system architecture modification. This master's thesis demonstrated the utilization of technology to tackle a real-world problem. Moreover, the connections between this study and several domains of knowledge, namely cascading effects, chemical and process facilities, and cybersecurity, have highlighted not only the connection of this study to various technological context but also showed the multidisciplinary nature of this study.

The second criterion of the study programme requires the master's thesis to adopt the perspective of corporations. There can be more than one type of problem owners of the main challenge being tackled in this master's thesis, such as the system owners, the governments, and others. The main perspective of this master's thesis is exhibited by the developed a risk management option that can be implemented by and may benefit the system owners as corporate entities. Moreover, this study has also gone further than the main objective to investigate the drawbacks that might entail from the implementation of network segmentation, in which the drawbacks are framed and analyzed as an added cost from the perspective of companies. Hence, in addition to presenting a practical solution for the main problem, this thesis also provides some analyses on whether the solution would be optimal from the perspective of corporations. Also, interviews with practitioners were also conducted to ensure the applicability of the proposed solution in corporate settings.

The last criterion mandates the use of scientific techniques and methods as introduced in MoT curriculum. The most apparent fulfillment of this criterion is exhibited within the discussion chapter. The first part took the perspective of cyber risk management where the findings are framed and discussed as a risk management strategy. Further, some risk management strategy alternatives which can be taken to tackle the same issue is compared to the proposed solution using a framework introduced in cyber risk management curriculum. In the second part, the findings are framed as a security investment decision and analyzed from the perspective of the economics of cybersecurity.

References

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D., & Abbasi, S. A. (2011). Domino effect in process-industry accidents–An inventory of past events and identification of some patterns. *Journal of Loss Prevention in the Process Industries, 24*(5), 575-593.

Agena Ltd. (2009). Retrieved from www.AgenaRisk.co.uk.

Ahmed, I., Obermeier, S., Naedele, M., & Richard III, G. G. (2012). Scada systems: Challenges for forensic investigators. *Computer, 45*(12), 44-51.

Albert, R., Jeong, H., & Barabási, A.-L. (2000). Error and attack tolerance of complex networks. *Nature, 406*(6794), 378.

ALOHA. (2016). Retrieved from https://www.epa.gov/cameo/aloha-software

Arturson, G. (1987). The tragedy of San Juanico—the most severe LPG disaster in history. *Burns, 13*(2), 87-102.

Asthana, A., & Elgot, J. (2016, 1 November 2016). Philip Hammond to spend extra £1.9bn fighting cyber-attacks. Retrieved from https://www.theguardian.com/technology/2016/nov/01/philp-hammond-to-spend-extra-19bn-fighting-cyber-attacks

Bailey, D., & Wright, E. (2003). *Practical SCADA for industry*: Newnes.

Barrett, C., Beckman, R., Channakeshava, K., Huang, F., Kumar, V. A., Marathe, A., . . . Pei, G. (2010). *Cascading failures in multiple infrastructures: From transportation to communication network.* Paper presented at the Critical infrastructure (CRIS), 2010 5th international conference on.

Battiston, S., Gatti, D. D., Gallegati, M., Greenwald, B., & Stiglitz, J. E. (2007). Credit chains and bankruptcy propagation in production networks. *Journal of Economic Dynamics and Control, 31*(6), 2061-2084.

BBC. (2006). Buncefield tank 'was overflowing'. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/4752819.stm

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D.-U. (2006). Complex networks: Structure and dynamics. *Physics reports, 424*(4), 175-308.

Bochman, A. (2018). Internet Insecurity. *Harvard Business Review.* Retrieved from https://hbr.org/2018/05/security-trends-by-the-numbers

Bologna, S., Fasani, A., & Martellini, M. (2013). Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures *Cyber Security* (pp. 57-72): Springer.

Boyes, H. (2013). Trustworthy cyber-physical systems-a review.

Candreva, F., De Rademaeker, E., Gowland, R., Isakov, A., Roberts, A., & Winkelmann-Oei, G. (2015). *Safety Guidelines and Good Industry Practices For Oil Terminals*. Retrieved from http://www.unece.org/index.php?id=41066

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). *Challenges for securing cyber physical systems.* Paper presented at the Workshop on future directions in cyber-physical systems security.

Clini, F., Roman, D., Maria, R., & Casal Fàbrega, J. (2010). Historical analysis of accidents involving domino effect. *Chemical Engineering Transactions, 19*, 335-340.

Cox, J., Louis Anthony. (2009). Game theory and risk analysis. *Risk Analysis: An International Journal, 29*(8), 1062-1068.

Cozzani, V., Gubinelli, G., Antonioni, G., Spadoni, G., & Zanelli, S. (2005). The assessment of risk caused by domino effect in quantitative area risk analysis. *Journal of hazardous materials, 127*(1), 14-30.

Crucitti, P., Latora, V., Marchiori, M., & Rapisarda, A. (2004). Error and attack tolerance of complex networks. *Physica A: Statistical Mechanics and its Applications, 340*(1), 388-394.

Csardi, G., & Nepusz, T. (2006). The igraph software package for complex network research. *InterJournal, Complex Systems, 1695*(5), 1-9.

De Bruijne, M., van Eeten, M., Gañán, C. H., & Pieters, W. (2017). Towards a new cyber threat actor typology.

Delvosalle, C. (1996). *Domino effects phenomena: definition, overview and classification.* Paper presented at the First European Seminar on Domino Effects.
Edwards, T. D. (2004). Using Network Segmentation to Optimize Network Performance. *Dell Power Solutions*, 133-136.
Exida, L. (2015). Repository of Industrial Security Incidents (RISI) Online Incident Database.
Fovino, I. N., Carcano, A., Masera, M., & Trombetta, A. (2009). An experimental investigation of malware attacks on SCADA systems. *International Journal of Critical Infrastructure Protection, 2*(4), 139-145.
Genge, B., & Siaterlis, C. (2012). *An experimental study on the impact of network segmentation to the resilience of physical processes.* Paper presented at the International Conference on Research in Networking.
Gertz, B. (2017, 14 June 2017). North Korea's hack threat. Retrieved from http://www.washingtontimes.com/news/2017/jun/14/north-korea-threatens-hack-to-attack-infrastructur/
Gledhill, J., & Lines, I. (1998). *Development of Methods to Access the Significance of Domino Effects from Major Hazard Sites*: HSE Books.
Hadžiosmanović, D. (2014). *The process matters: cyber security in industrial control systems*: University of Twente.
Hayden, E., Assante, M., & Conway, T. (2014). An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity. *SANS Analyst White Papers*.
Honeywell. (2011). *Effectively applying the total cost of ownership equation to the process automation industries [White paper]*. Retrieved from https://www.plantservices.com/assets/Media/1106/total-cost-of-ownership-equation.PDF
ICS-CERT, & NCCIC. (2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
Johnston, C., Russell, G., Levin, S., Wong, J. C., & Rawlinson, K. (2017). Disruption from cyber-attack to last for days, says NHS Digital – as it happened. Retrieved from https://www.theguardian.com/society/live/2017/may/12/england-hospitals-cyber-attack-nhs-live-updates?page=with:block-59162e84e4b0f5ae171e1a6d
Khakzad, N. (2015). Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. *Reliability Engineering & System Safety*, *138*, 263-272.
Khakzad, N., Khan, F., Amyotte, P., & Cozzani, V. (2013). Domino effect analysis using Bayesian networks. *Risk Analysis, 33*(2), 292-306.
Khakzad, N., Landucci, G., Cozzani, V., Reniers, G., & Pasman, H. (2018). Cost-effective fire protection of chemical plants against domino effects. *Reliability Engineering & System Safety*, *169*, 412-421.
Khakzad, N., & Reniers, G. (2015). Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. *Reliability Engineering & System Safety*, *143*, 63-73.
Khakzad, N., & Reniers, G. (2018). Low-capacity utilization of process plants: A cost-robust approach to tackle man-made domino effects. *Reliability Engineering & System Safety*.
Khakzad, N., Reniers, G., Abbassi, R., & Khan, F. (2016). Vulnerability analysis of process plants subject to domino effects. *Reliability Engineering & System Safety*, *154*, 127-136.
Khan, F. I., & Abbasi, S. (1998). Models for domino effect analysis in chemical process industries. *Process Safety Progress, 17*(2), 107-123.
Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005). Modeling cascading failures in the North American power grid. *The European Physical Journal B-Condensed Matter and Complex Systems, 46*(1), 101-107.
Knapp, E. D., & Langill, J. T. (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*: Syngress.
Koç, Y., Warnier, M., Kooij, R. E., & Brazier, F. M. (2013). *A robustness metric for cascading failures by targeted attacks in power networks.* Paper presented at the Networking, Sensing and Control (ICNSC), 2013 10th IEEE International Conference on.
Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2011). *Interdependencies between critical infrastructures: Analyzing the risk of cascading effects.* Paper presented at the International Workshop on Critical Information Infrastructures Security.
Kozak, A., Kościelny, M., Pacyna, P., Gołębiewski, D., Paturej, K., & Świątkowska, J. (2016). *Cybersecurity and Industrial Plants – Foundation of the "Industry 4.0" Project and a Chance for Poland*. Retrieved from https://2017.cybersecforum.eu/white-paper-

cybersecurity-and-industrial-plants-foundation-of-the-industry-4-0-project-and-a-chance-for-poland/
Kramer, A. E. (2016, 29 December 2016). How Russia Recruited Elite Hackers for Its Cyberwar. Retrieved from https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html
Krotofil, M., & Gollmann, D. (2013). *Industrial control systems security: What is happening?* Paper presented at the Industrial Informatics (INDIN), 2013 11th IEEE International Conference on.
Krotofil, M., & Larsen, J. (2015). *Rocking the pocket book: Hacking chemical plants.* Paper presented at the DefCon Conference, DEFCON.
Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49-51.
Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber attack. *Industrial Control Systems, 30*.
Lennon, M. (2013). Cyber Attacks Targeted Key Components of Natural Gas Pipeline Systems. Retrieved from https://www.securityweek.com/cyber-attacks-targeted-key-components-natural-gas-pipeline-systems
Lewis, P., & Macalister, T. (2010). Buncefield fire: Oil storage firm found guilty of safety breaches. Retrieved from https://www.theguardian.com/uk/2010/jun/18/buncefield-fire-oil-company-guilty
Lim, A. (2017, 2017, March 4th). Singapore strengthens cyber defence with new organisation. Retrieved from http://www.straitstimes.com/singapore/spore-strengthens-cyber-defence-with-new-organisation
Martellini, M. (2013). *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*: Springer.
Matches. (2014). Retrieved from http://matche.com/equipcost/Tank.html
McMillan, R. (2018, 19 Jan 2018). New Type of Cyberattack Targets Factory Safety Systems. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/hack-at-saudi-petrochemical-plant-compromised-a-safety-shut-off-system-1516301692
Metivier, B. (2017). The Security Benefits of Network Segmentation. Retrieved from https://www.sagedatasecurity.com/blog/the-security-benefits-of-network-segmentation
Miller, C. (2006). *Security Considerations in Managing COTS Software*. Retrieved from
Ministerie van Veiligheid en Justitie. (2015). *Voortgangsbrief Nationale Veiligheid*. Retrieved from www.rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/05/14/tk-voortgangsbrief-nationale-veiligheid
Mittal, A., Slaughter, A., & Zonneveld, P. (2017). Protecting the connected barrels: Cybersecurity for upstream oil and gas. Retrieved from https://dupress.deloitte.com/dup-us-en/industry/oil-and-gas/cybersecurity-in-oil-and-gas-upstream-sector.html
Moreno, V. C., Reniers, G., Salzano, E., & Cozzani, V. (2018). Analysis of physical and cyber security-related events in the chemical and process industry. *Process safety and environmental protection, 116*, 621-631.
Morsi, I., & El-Din, L. M. (2014). SCADA system for oil refinery control. *Measurement, 47*, 5-13.
Motter, A. E., & Lai, Y.-C. (2002). Cascade-based attacks on complex networks. *Physical Review E, 66*(6), 065102.
Nicholas, P. (2017). Mind the air gap: Network separation's cost, productivity and security drawbacks. Retrieved from https://www.microsoft.com/en-us/cybersecurity/blog-hub/mind-the-air-gap-network-separation
North American Electric Reliability Council. (2005). *Evaluation of Criteria, Methods, and Practices Used for System Design, Planning, and Analysis Response to NERC Blackout Recommendation 13c*. Retrieved from http://www.nerc.com/docs/pc/tis/AppC_Regional_Summaries_Recom_13c.pdf
Packham, C. (2017, 30 June 2017). Australia creates military cyber unit to expand hacking attacks. Retrieved from http://www.channelnewsasia.com/news/technology/australia-creates-military-cyber-unit-to-expand-hacking-attacks-8991598
Park, J.-m., & Pearson, J. (2017, 21 May 2017). Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West. Retrieved from http://www.reuters.com/article/us-cyber-northkorea-exclusive-idUSKCN18H020

Perlroth, N., & Krauss, C. (2018, 15 March 2018). A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try. *The New York Times.* Retrieved from https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
Reed, T. C. (2005). *At the abyss: an insider's history of the Cold War*: Presidio Press.
Reniers, G., & Cozzani, V. (2013). *Domino effects in the process industries: modelling, prevention and managing*: Newnes.
Reniers, G., & Faes, R. (2013). Managing domino effects in a chemical industrial area *Domino Effects in the Process Industries* (pp. 272-295): Elsevier.
Reniers, G. L. (2010). *Multi-plant safety and security management in the chemical and process industries*: John Wiley & Sons.
Reniers, G. L., & Audenaert, A. (2014). Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures wrt domino effects. *Process safety and environmental protection, 92*(6), 583-589.
Reniers, G. L., & Dullaert, W. (2008). Knock-on accident prevention in a chemical cluster. *Expert systems with applications, 34*(1), 42-49.
Rew, P., & Daycock, L. (2004). Development of a method for the determination of on-site ignition probabilities, HSE Contractor Report WSA/226: HSE Books, London, UK.
Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11-25.
Sahasrabudhe, S., & Motter, A. E. (2011). Rescuing ecosystems from extinction cascades through compensatory perturbations. *arXiv preprint arXiv:1103.1653*.
Sanger, D. E. (2012). Obama order sped up wave of cyberattacks against Iran. *The New York Times*, 2012.
Schmidt, M. S., & Perlroth, N. (2013). Obama Order Gives Firms Cyberthreat Information. Retrieved from http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html
Security Roundtable. (2018). 'Tried and True' Network Segmentation Can Come to the Rescue. Retrieved from https://www.securityroundtable.org/tried-true-network-segmentation-can-come-rescue/
Siemens. (2008). *Security concept PCS 7 and WinCC - Basic document (Whitepaper)*. Retrieved from https://cache.industry.siemens.com/dl/files/131/26462131/att_80283/v1/wp_sec_b.pdf
Srivastava, A., & Gupta, J. (2010). New methodologies for security risk assessment of oil and gas industry. *Process safety and environmental protection, 88*(6), 407-412.
Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. Risk management guide for information technology systems. *NIST special publication*.
Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication, 800*(82), 16-16.
The Washington Times. (2004, 12 October 2004). Chinese information warfare threatens Taiwan. Retrieved from http://www.washingtontimes.com/news/2004/oct/12/20041012-101455-7846r/
Trend Micro. (2016). Industrial Control System. Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system
U.S. Department of Homeland Security. (2017, 11 July 2017). Critical Infrastructure Sectors. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors
U.S.-Canada Power System Outage Task Force. (2004). *Final Report on the August 14th Blackout in the United States and Canada*. Retrieved from https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf
US Department of Homeland Security. (2004). *FOIA Documents: Control Systems Security Aurora Update Brief*. Retrieved from Washington, DC: http://s3.documentcloud.org/documents/1212530/14f00304-documents.pdf
Usborne, D. (1998). Satellite's failure leaves millions speechless in US. Retrieved from http://www.independent.co.uk/news/satellites-failure-leaves-millions-speechless-in-us-1157828.html
Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., & Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. *Public Administration, 89*(2), 381-400.
Vinnem, J.-E. (2014). Approach to Risk Based Design *Offshore Risk Assessment vol 2.* (pp. 717-744): Springer.

Volz, D. (2017). Trump signs order aimed at upgrading government cyber defenses. Retrieved from http://www.reuters.com/article/us-usa-trump-cyber-idUSKBN1872L9

Wagner, N., Sahin, C. S., Pena, J., & Streilein, W. W. (2017). *A nature-inspired decision system for secure cyber network architecture.* Paper presented at the Computational Intelligence (SSCI), 2017 IEEE Symposium Series on.

Wang, J., Jiang, C., & Qian, J. (2014). Robustness of Internet under targeted attack: A cascading failure perspective. *Journal of Network and Computer Applications, 40*, 97-104.

Wang, J., Rong, L., Zhang, L., & Zhang, Z. (2008). Attack vulnerability of scale-free networks due to cascading failures. *Physica A: Statistical Mechanics and its Applications, 387*(26), 6671-6678.

Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence, 25*(4), 671-682.

White, K., & Bickley, M. (2001). *Control system segmentation.* Paper presented at the Particle Accelerator Conference, 2001. PAC 2001. Proceedings of the 2001.

Zeitlin, A. (2018). The hidden costs of VLAN segmentation. Retrieved from https://www.guardicore.com/2018/07/hidden-cost-vlan-segmentation/

Zeller, M. (2011). *Myth or reality-does the aurora vulnerability pose a risk to my generator.* Paper presented at the Protective Relay Engineers, 2011 64th Annual Conference for.

Zhao, L., Park, K., & Lai, Y.-C. (2004). Attack vulnerability of scale-free networks due to cascading breakdown. *Physical Review E, 70*(3), 035101.

This page intentionally left blank

Appendix A

Chemical Facilities and Storage Tanks Overview

Being the main context of this study, it is essential to have an understanding about what kind of facility chemical plants and storage tanks are, what are they composed of, and what sort of activities undertaken in these facilities.

The Department of Homeland Security (DHS) of the United States defines facilities in the chemical sector as the facilities that manufacture, store, consume, and distribute potentially hazardous chemicals that might be required by a wide range of other critical infrastructures. Some examples of end products from chemical plants including basic chemicals, pharmaceutical, and consumer products. Oil refineries sometimes also considered as chemical plants.

The importance of chemical plants cannot be understated. DHS stated that the 70,000 diverse products from chemical facilities are essential to the society. In Europe, the European Union also acknowledge the importance of chemical plants. In 2013, the chemical industry in Europe accounted for seven percent of EUs industrial production with more than 1.15 million employment.

Interestingly, several countries have differently classified chemical plants as critical infrastructures. The United States Department of Homeland Security includes the chemical sector among the sixteen sectors it recognizes as critical infrastructures. The UK Government classifies chemical sector among thirteen critical national infrastructure (CNI) sectors. The European Union, through Council Directive 2008/114/EC, has suggested the classification of critical infrastructures for its member states. Although the directive does not specifically mention chemical plant, oil and gas facilities are included among the proposed list of critical infrastructure sectors. The directive is more of guidance than instruction since the process of selection and protection of critical infrastructures are responsibilities of each member state. The Ministry of Security and Justice of the Dutch Government does not classify chemical plants as critical infrastructures but specifically mentions oil supply facilities in the energy sector and large-scale production and storage of petrochemicals as critical infrastructures.

Chemical Storage Tanks

One type of chemical plant is the chemical storage tank (or storage tank), which is a massive container used to store various chemical substance temporarily. Storage tanks are typically a cylindrically shaped container that is placed perpendicular to the ground. Different other shapes have also been used, such as spherical and horizontal-cylindrical shape. These tanks are usually large with a capacity ranging from 12,000 liters to more than 178 million liters, and their diameters vary from three meters to 125 meters. Various materials are used to manufacture these tanks, but stainless steel and concrete are the two most used materials. Storage tanks are usually found in white to reflect heat from outside and therefore minimize the change of temperature inside the tanks. When a lot of storage tanks are placed close together in one area, then the storage tank complex is usually called a tank farm. Tank farms commonly found located nearby some refinery facilities.

Figure 44. An example of typical storage tanks

There are several types of storage tanks. One classification distinguishes between atmospheric storage tanks and high-pressure storage tanks. As the name suggests, atmospheric storage tanks (or low-pressure storage tanks) are the types of tanks that store liquid chemicals at atmospheric pressure. On the other hand, high-pressure storage tanks are used to store various kinds of chemicals at high pressure, such as gases and liquefied gases. High-pressure tanks are designed to withstand enormous pressure from the interior of the tanks. Atmospheric tanks can be divided into several more categories, namely floating roof tanks and fixed roof tanks. While fixed roof tank will always stay in the same shape, floating roof tanks allow the ceiling of the tank to move up-and-down depending on the level of the content. One of the primary purposes of employing floating roof is to minimize the buildup of vapor in various flammable chemicals. There are still several types of storage tanks, such as underground and aboveground tanks, refrigerated tanks, insulated and uninsulated tanks, and others.

In addition to the tanks, there is also a group of devices called ancillary equipment. Several ancillary equipment that are typically present in storage tanks facility are pipework, valves, pumps, measurement and gauging devices, etc.

Table 33. Examples of ancillary equipment in chemical plants

Name	Type	Description
Pipework	–	The network of pipes that connect different components in the chemical facilities.
Valve	Actuator	To direct the flow of chemical liquids or gases from one component to another through the pipework. Typically there are a number of valves in a facility and this set of valves need to be configured in such a way as to set the flow direction of the chemical cargo as intended.
Pump	Actuator	Create a pressure difference in the pipework which forces the chemical product to flow the determined direction.
Gauging and measurement tools	Sensor	Indicate which tanks are empty, how much the flow rate, whether a tank is full or not, etc. Some measured metrics include flow rate, temperature and pressure, and product volume in the tank.

Activities and Operations Involving Storage Tanks

The activities in chemical storage tanks revolve around transferring and storing different kinds of liquid products. There is the unloading activity, or also called discharging, which is the process of receiving payload or cargo from supply links to storage tanks. Supply links may refer to vessels, pipelines, rail, or truck tankers. Although it might seem counterintuitive to associate the term "unloading" as the process of "filling" a storage tank, it can be easily understood by recognizing that these terms are established from the perspective of the supply links operator (vessel, rail, trucks, etc.). Conversely, loading is the activity in which the payload or cargo is transferred from storage tanks to supply links. Storage tanks generally discharge payload to truck tankers, vessels, or pipelines. So, for instance, unloading may refer to the transfer of liquids from a vessel to a storage tank, while loading may refer to the transfer from storage tanks to truck tankers.

Loading and unloading activities are composed of other activities. For unloading activity, or also called discharge or filling operations, the typical first step is valve adjustment. This task includes opening and closing particular valves to a certain arrangement according to the intended operation. After the valves are set in the intended configuration, the next step is to operate the pump to move the liquid product until the filling process is finished. Valve adjustment and pump operation are among the major tasks undertaken during the loading and unloading operations. The loading (or draining) operation consists of a similar set of tasks with a slight variation. In the modern days, the loading and unloading operation can be done and monitored remotely through computerized systems. Tasks such as adjusting valve, turning a pump on and off, and pressure and temperature monitoring, all can be done from a remote location by using computerized systems.

Candreva et al. (2015) categorized the operations of storage tanks into routine tasks and non-routine tasks. Unloading/discharging, loading, and transfer activities are categorized as routine tasks. Some examples of non-routine tasks are the removal of the pressure safety valve. Although loading and unloading are the typical operations in storage tanks, research has indicated that a significant portion of spill incidents occur during loading and unloading activities. According to analysis from ITOPF (2017), loading and unloading operations account for 40% of small spills and 29% of medium spills. This percentage is relatively higher than the other activities. This statistic indicates that loading and unloading operations are still risky operations.

This page intentionally left blank

Appendix B

Bayesian network for Attack Scenario 2 in NSD-26.

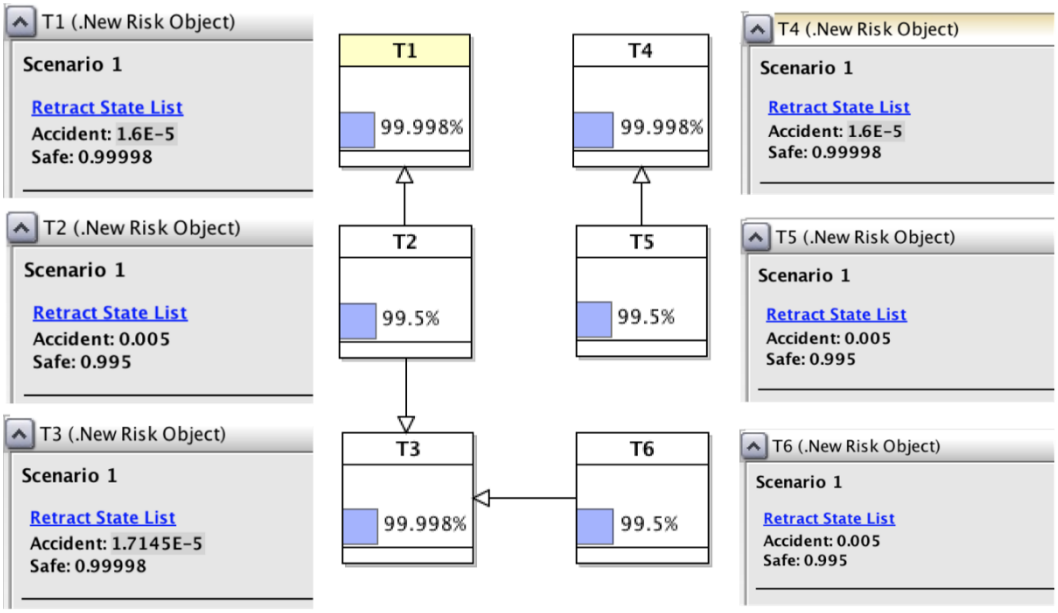


Figure 45. Bayesian-network for At_2 scenario in NSD-26

This page intentionally left blank

Appendix C

Graph metric analysis using R.

```
library(igraph)

# build storage tank graph
storagetank <-
graph(edges=c("T1","T2","T1","T4","T2","T1","T2","T5","T2","T3","T3","T2","T3","T6","T
4","T1","T4","T5","T5","T4","T5","T2","T5","T6","T6","T3","T6","T5"), directed=TRUE)

E(storagetank)["T1|T2"]$weight <- 0.395
E(storagetank)["T1|T4"]$weight <- 0.682
E(storagetank)["T2|T1"]$weight <- 0.395
E(storagetank)["T2|T5"]$weight <- 0.682
E(storagetank)["T2|T3"]$weight <- 0.395
E(storagetank)["T3|T2"]$weight <- 0.395
E(storagetank)["T3|T6"]$weight <- 0.682
E(storagetank)["T4|T1"]$weight <- 0.682
E(storagetank)["T4|T5"]$weight <- 0.395
E(storagetank)["T5|T4"]$weight <- 0.395
E(storagetank)["T5|T2"]$weight <- 0.682
E(storagetank)["T5|T6"]$weight <- 0.395
E(storagetank)["T6|T3"]$weight <- 0.682
E(storagetank)["T6|T5"]$weight <- 0.395

# centrality calculation
print(degree(storagetank, mode="out"))
print(closeness(storagetank))
print(betweenness(storagetank))

# draw graph
plot(storagetank)
```

This page intentionally left blank

Appendix D

In this section, the application of the BN method and the subsequent risk assessment process for one of the network segmentation design alternatives in Chapter 7 is described. This section presents a risk assessment for At_1 in NSD-3 (see Figure 46 below).

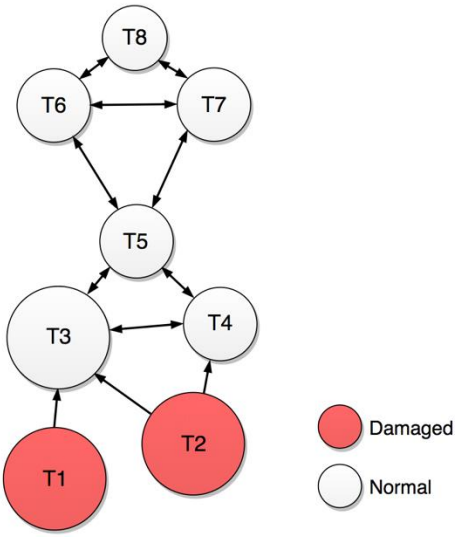


Figure 46. Illustration of the primary units in Attack Scenario 1 of NSD-3

Firstly, to calculate the damage probability of each storage tank, a BN for the attack scenario must be developed. For this purpose, the structure of the BN is developed by determining the propagation of accidents. The first step is to calculate the potential escalation vectors and the potential escalation probabilities. The potential escalation vectors between the storage tanks have been calculated and presented in Table 28 (page 88). Using the equations Eq. 12, Eq. 13, and Eq. 14, the escalation probabilities can be calculated based on the escalation vectors value in Table 28. The following tables present the escalation probability calculation for At_1 in NSD-3.

Table 34. Escalation vectors and escalation probabilities of potential secondary units for At_1 scenario in NSD-3

Ti → Tj	**Escalation Vector**	**Escalation Probability**
T1, T2 → T3	**53 kW/m^2**	**3.17×10^{-1}**
T2 → T4	19 kW/m^2	4.55×10^{-4}

From Table 34, it can be seen that escalation probability toward T3 is higher than that of T4. Therefore, T3 is determined as the secondary unit, and the step is repeated to determine the tertiary units, quaternary units, quinary units, etc.

Table 35. Escalation vectors and escalation probabilities of potential tertiary units for At_1 scenario in NSD-3

Ti → Tj	**Escalation Vector**	**Escalation Probability**
T2, T3 → T4	**53 kW/m^2**	**1.190×10^{-1}**
T3 → T5	34 kW/m^2	1.77×10^{-2}

Table 36. Escalation vectors and escalation probabilities of potential quaternary units for At_1 scenario in NSD-3

Ti → Tj	**Escalation Vector**	**Escalation Probability**
T3, T4 → T5	**64 kW/m^2**	**2.16×10^{-1}**

Table 37. Escalation vectors and escalation probabilities of potential quinary units for At_1 scenario in NSD-3

Ti → Tj	**Escalation Vector**	**Escalation Probability**
T5 → T6	**15 kW/m^2**	**6.96×10^{-5}**
T5 → T7	**15 kW/m^2**	**6.96×10^{-5}**

A special note needs to be made for the quinary units: as the escalation probabilities from T5 to T6 and T5 to T7 are equal, both T6 and T7 are considered as the quinary units.

Table 38. Escalation vectors and escalation probabilities of potential senary units for At_1 scenario in NSD-3

Ti → Tj	**Escalation Vector**	**Escalation Probability**
T6, T7 → T8	**64 kW/m^2**	**1.21×10^{-1}**

Once the escalation probabilities for all units are calculated, the propagation of accidents can be determined. Figure 47 illustrates the propagation of accident for At_1 of NSD-3.

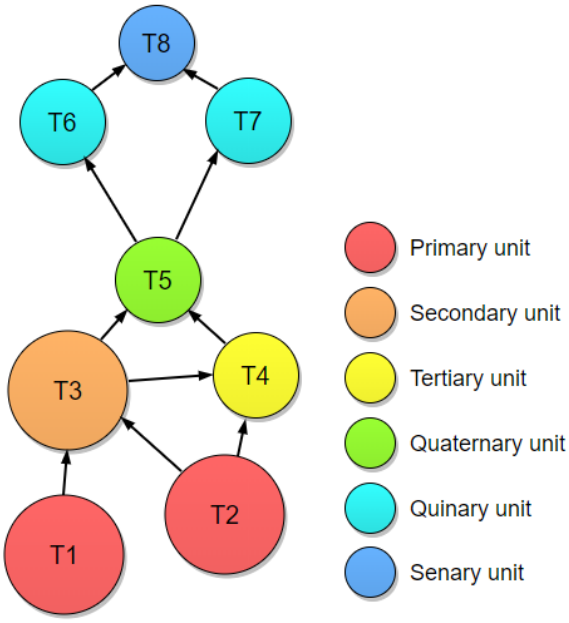


Figure 47. Illustration of the accident propagation for At_1 scenario in NSD-3

The next part is to develop the CPTs of the nodes as the quantitative part of the BN. Below are the CPTs for every node in the tank farm for At_1 of NSD-3.

Table 39. CPT of node T2 for At_1 scenario in NSD-3

T1	**T3**	**P(T2 = Fire | T1, T3)**	
		Accident	**Safe**
Accident	Accident	9.98×10^{-2}	0.90
Accident	Safe	3.20×10^{-3}	0.99
Safe	Accident	3.20×10^{-3}	0.99
Safe	Safe	0	1

Table 40. CPT of node T3 for At_1 scenario in NSD-3

T1	**T2**	**P(T3 = Fire | T1, T2)**	
		Accident	**Safe**
Accident	Accident	3.172×10^{-1}	6.828×10^{-1}
Accident	Safe	8.071×10^{-2}	9.193×10^{-1}
Safe	Accident	4.491×10^{-3}	9.955×10^{-1}
Safe	Safe	0	1

Table 41. CPT of node T4 for At_1 scenario in NSD-3

T2	T3	P(T4 = Fire | T2, T3)	
		Accident	Safe
Accident	Accident	1.190×10^{-1}	8.810×10^{-1}
Accident	Safe	1.766×10^{-2}	9.823×10^{-1}
Safe	Accident	4.547×10^{-4}	9.995×10^{-1}
Safe	Safe	0	0

Table 42. CPT of node T5 for At_1 scenario in NSD-3

T3	T4	P(T5 = Fire | T3, T4)	
		Accident	Safe
Accident	Accident	2.157×10^{-1}	7.843×10^{-1}
Accident	Safe	1.766×10^{-2}	9.823×10^{-1}
Safe	Accident	9.002×10^{-3}	9.910×10^{-1}
Safe	Safe	0	0

Table 43. CPT of node T6 for At_1 scenario in NSD-3

T5	P(T6 = Fire | T5)	
	Accident	Safe
Accident	6.959×10^{-5}	9.999×10^{-1}
Safe	0	0

Table 44. CPT of node T7 for At_1 scenario in NSD-3

T5	P(T7 = Fire | T5)	
	Accident	Safe
Accident	6.959×10^{-5}	9.999×10^{-1}
Safe	0	0

Table 45. CPT of node T8 for At_1 scenario in NSD-3

T6	T7	P(T8 = Fire | T6, T7)	
		Accident	**Safe**
Accident	Accident	1.208×10^{-1}	8.792×10^{-1}
Accident	Safe	4.458×10^{-3}	9.955×10^{-1}
Safe	Accident	4.458×10^{-3}	9.955×10^{-1}
Safe	Safe	0	0

After the CPTs for all the nodes have been developed, the BN model for the attack scenario can be developed. The BN for At_1 of NSD-3 is developed using AgenaRisk software (Agena Ltd., 2009), and the result is presented in Figure 48. From the BN, the probability of damage for every node can be estimated. Accordingly, the risk for every storage tank can be calculated by multiplying the probability of damage with the cost of the storage tank (see Table 30). Finally, the risk level for the attack scenario can be calculated by summing up the risk of each storage tank.

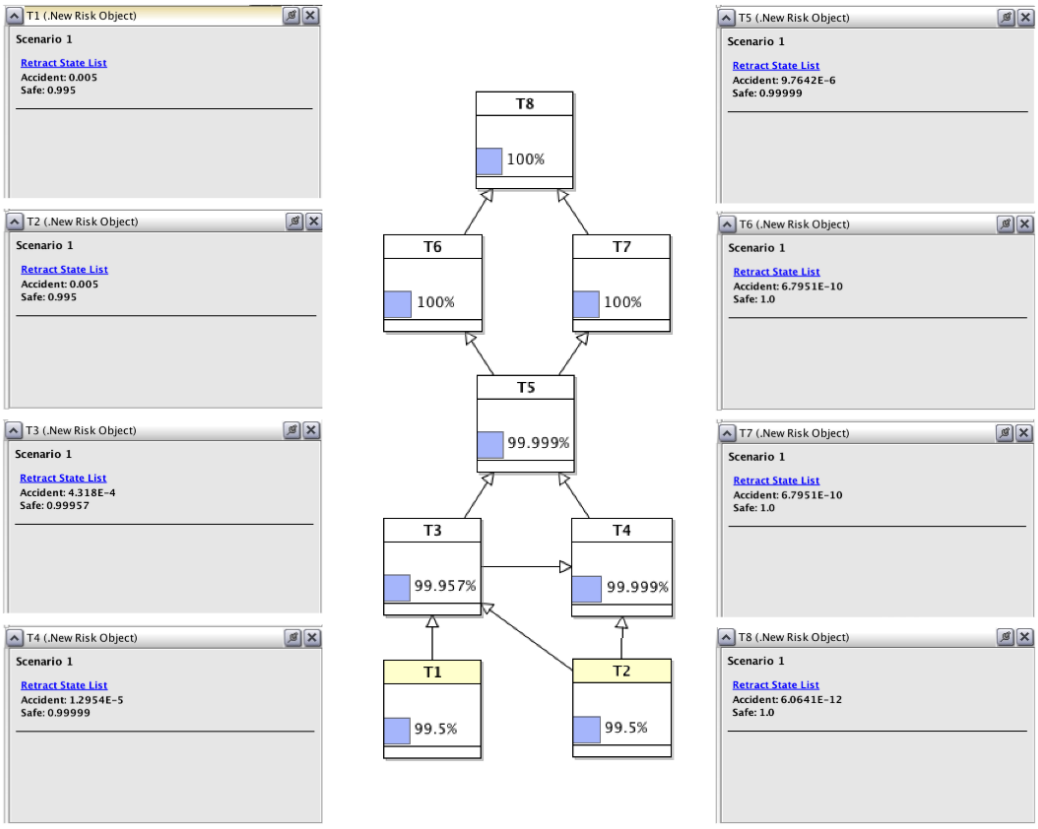


Figure 48. BN for At_1 scenario in NSD-3. T1 and T2 are the primary units.

Table 46. Risk of damage for the storage tanks in At_1 of NSD-3

Storage tank	Probability of Accident	Risk
T1	5.000×10^{-3}	€ 10,287.50
T2	5.000×10^{-3}	€ 10,287.50
T3	4.318×10^{-4}	€ 888.43
T4	1.295×10^{-5}	€ 21.22
T5	9.764×10^{-6}	€ 16.00
T6	6.795×10^{-10}	€ 0.00
T7	6.795×10^{-10}	€ 0.00
T8	6.064×10^{-12}	€ 0.00
Total		**€ 21,500.65**

Appendix E

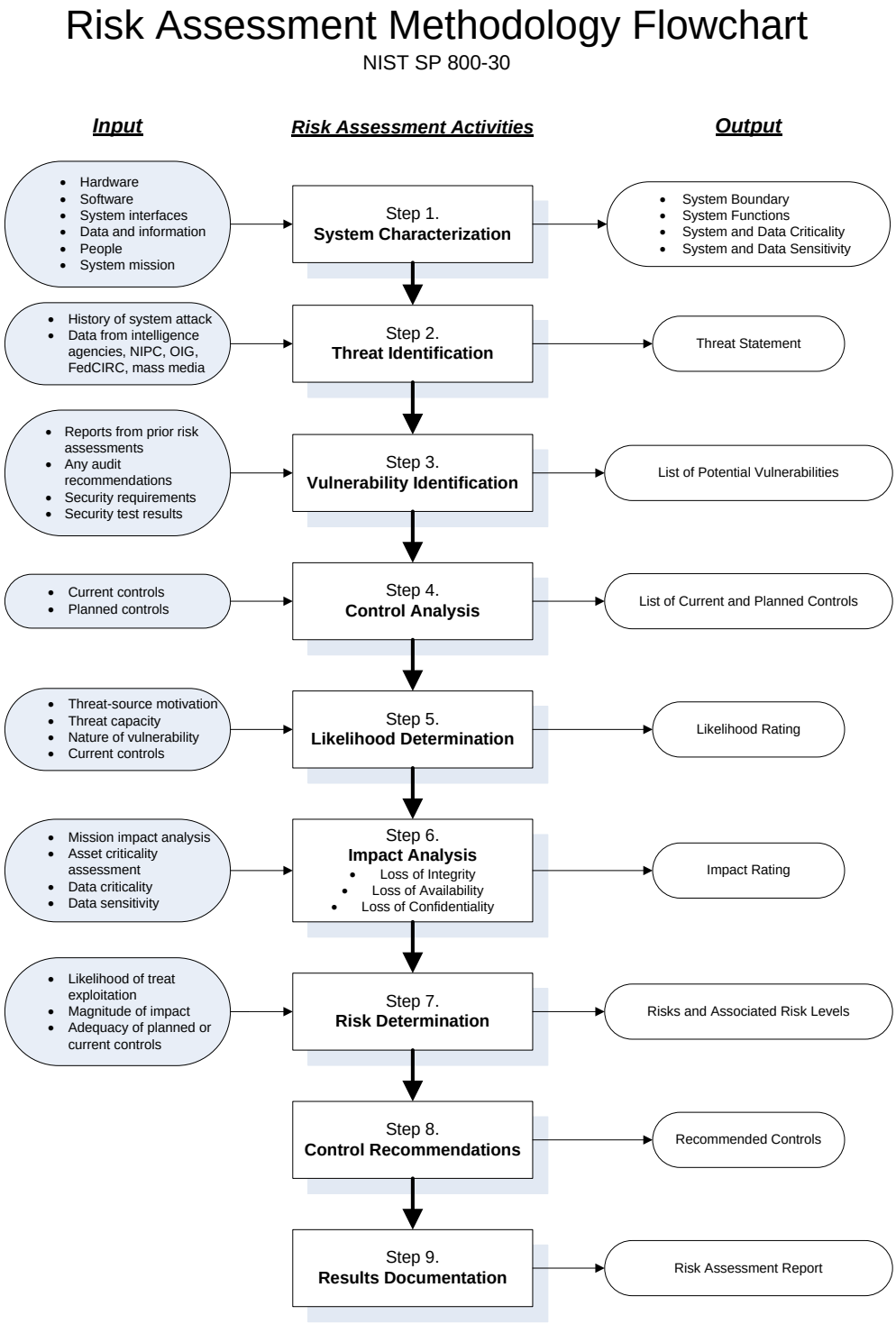


Figure 49. Flowchart of NIST's risk assessment steps (Stoneburner et al., 2002)