Using Publicly Available Information to Predict Cyber Failures

Parisa Badalkhani

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirement for the degree of the

Master of Applied Science

in

Technology Innovation Management

Faculty of Engineering and Design

Carleton University

Abstract

This research examines the use of an anticipatory method and publicly available newsworthy information on ten past cyber failures of critical infrastructures in the United States to predict cyber failures of networks and systems of technology startups.

The Anticipatory Failure Determination (AFD) method was modified to enable the use of publicly available information. A list of the resources that were used to cause the ten cyber failures in critical infrastructures was produced and used to make predictions of failure scenarios of a stack of open source software. Finally, the factors that enable and constrain the use of the AFD method to predict cyber failures in technology startups were specified.

Junior engineers, designers, contractors and other stakeholders of cyber systems as well as government policy makers will be interested in outcome of this research to predict potential cyber failures for proactive mitigation.

Acknowledgement

Firstly, I would like to express my sincere gratitude to my advisor Prof. Bailetti for the continuous support, for his patience, motivation, and immense knowledge. I could not have imagined having a better advisor and mentor for my study.

I would like to thank my professors: Prof. Craigen, Prof. Weiss, Prof. Muegge, and Prof. Westerlund for their supports and precious ideas for improving this study.

I deeply grateful to my family: my parents, my brothers, and sister for supporting me spiritually throughout my life.

I must express my very profound gratitude to my spouse, Hamidreza and my sweetheart, Parham for their understanding and unfailing encouragement throughout my years of study. This accomplishment would not have been possible without them. Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

1.1 Motivation

Three factors motivated this research. The desire to predict cyber failures of the systems and networks of technology startups worldwide by building on recent advances made to predict cyber failures of critical infrastructures in North America was the first factor that motivated this research. Precedents for building on the knowledge gained protecting critical infrastructures to protect small businesses exist. For example, the Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology, 2014) was developed through collaboration of the United States federal government and industry over decades. The framework organizes the processes and tools that provide the key standards and best practices that presently protect the critical infrastructures in the United States. While the framework was originally developed specifically for critical infrastructures, it has been used to develop a guide to help small businesses provide basic security for their information, systems, and networks (National Institute of Standards and Technology, 2016).

The second factor that motivated this research was the desire to fill a knowledge gap identified in the academic literature: how to predict cyber failures using an anticipatory method and publicly available information on past cyber failures. To make cyber failure predictions, most processes use secret or restrictive information. To the knowledge of the researcher and her supervisor, studies that report on the application of an anticipatory method to predict and mitigate cyber failures using publicly available

information about resources that contributed to past cyber failures have not been published. The prevalent use of secret or restricted information to make cyber failure predictions prevents the development of online resources that maintain data on past failures of critical infrastructure and non-critical infrastructure systems at a global scale.

The third factor that motivated this research was the prospect that knowledge gained predicting cyber failures of technology startups linked by global ecosystems could be used to predict failures of critical infrastructures and a variety of non-critical infrastructures. Presently, the academic and professional literature on predicting cyber failures of critical infrastructure is better developed than the literature on predicting failures of systems and networks of technology startups and other non-critical infrastructure systems. The day may come when rapid advances in the literature on predicting cyber failures of technology startups will offer benefits to the extant literature.

1.2 Prediction Method

Predicting cyber failures of a system likely to or liable to suffer from cyberattacks, requires a process and information about past cyber failures (Teixeira et al., 2015). The processes used to predict cyber failures depend on methods that can be organized into traditional risk analysis methods and anticipatory methods.

Traditional risk analysis methods used to predict cyber failures of critical infrastructure include HAZOP, HAZID, fault tree, scenario tree, and event tree analysis (Ahmed et al., 2007; Dunjó et al., 2010). These traditional risk analysis methods use

linear inductive thinking or logical modeling to answer questions such as "How did this failure happen?" or “How can this failure happen?” (Zio, 2016 a,b).

The researcher selected the Anticipatory Failure Determination (AFD) method for carrying out the research for two reasons. First, the application of the AFD to protect critical infrastructures has been gaining momentum recently. Boyes (2013), Clothier and Walker (2015), Gay and Sinha (2012), Masys (2012), and Zio (2016 a, b) suggest the use of the AFD method to predict and mitigate cyber failures in critical infrastructure.

The second reason for selecting the AFD method is because of the experience that exists using it to predict failures in manufacturing processes. The AFD method considers the information about past failures, their systems, and details of existing systems which are accessible online. Users of the AFD method identify the set of resources that contributed to a past failure – without one of the resources the failure could have not occurred (Kaplan et al., 1999; Proseanic et al., 2000; Sunday, 2014; Regazzoni and Russo, 2010).

AFD is a risk assessment method that systematically predicts and mitigates failure scenarios from a different perspective than the one used to carry out traditional failure analysis (Masys, 2012). The AFD method captures topological, functional, static and dynamic cyber failures that traditional risk analysis methods do not (GhasemiGol et al., 2016; Kröger & Zio, 2011; Kwon and Hwang, 2016; Rawal et al., 2016). AFD uses the knowledge gained from previous failures and experiences to provide answers to questions

such as “If I wanted to create this failure, how could I do it?" AFD addresses the means that cause a known failure to occur and the means that can cause unknown failures.

Kaplan et al. (1999) introduced the AFD method and suggested its use to examine cases of human errors, sabotage, and terrorism. AFD is based on I-TRIZ, a Russian short form of the theory of inventive problem solving (Sunday, 2014). The AFD extracts information about the resources that contributed to a failure (Masys, 2012) and mitigates occurrence of failure scenarios, by making explicit the knowledge about the failures and mitigation methods and disseminating it (Kaplan et al., 1999).

1.3 Goal, research question and objectives

The goal of this research is to identify the factors that enable and constrain the use of the AFD method and publicly available information on past cyber failures of critical infrastructures to predict cyber failures of technology startups.

The research question of this thesis is “how to use publicly available information about past failures in critical infrastructures to predict cyber failures of technology startups?”

The objectives of this research are:

1) Identify the components of the AFD method that can be used to predict cyber failures using publicly available information

2) Develop an anticipatory process to predict failures of non-critical infrastructure systems using publicly available information about past cyber failures in critical infrastructures
3) Predict cyber failures in a target system of a technology startup using the anticipatory process developed

1.4 Deliverables

The deliverables of this research include:

1) A resource knowledge inventory – a list of the resources that were used to cause failures in critical infrastructures over the last ten years.
2) An anticipatory process to predict cyber failures of non-critical infrastructure systems that uses publicly available information about past critical infrastructures failures.
3) Predictions of failure scenarios of LTW-Start, a stack of open source software.
4) Identification of the factors that enable and constrain the use of AFD and publicly available information to predict cyber failures.

1.5 Relevance

This research will be relevant to the stakeholders of cyber infrastructures as well as the operators of the nodes that distribute and support LTW-Start, the system that was used to make predictions of cyber failures.

Stakeholders of cyber infrastructure include operators, suppliers, open source communities, contractors and other organizations that affect or affected by cyber infrastructures. This research is relevant to these stakeholders because it is initiating

anticipatory thinking “to find the failures before they find us” (Kaplan et al., 1999). Anticipating failures in cyber infrastructures enables stakeholders to take proactive action to cost-effectively mitigate them.

This research is relevant to the engineers who design systems prone to cyberattacks because it increases awareness of how a weak design and bugs in systems may have a significant adverse impact on systems and collective of systems. Deliverables assist to predict failures autonomously from individual experience and knowledge, by transmitting the most recent worldwide experience about failures in critical infrastructures and non-critical systems that is publicly available.

This research is relevant to government policy makers because it provides a process to use publicly available information to predict and invent potential failures in different systems which can help shape future standards and policies for the purpose of mitigating the risk of future cyber failures.

The production and dissemination of an inventory of resources that contributed to the past failures of critical infrastructure around the world can raise awareness of cyber threats and increases capability to anticipate future failures.

The organizations that are part of the GCR network and open sources communities will find this research relevant. These node operators and open source communities are developing a fusion centre to mitigate cyber failures of LTW-Start.

1.6 Contribution

The main academic contribution of this research is to fill a knowledge gap identified in the literature- How to predict failures using the AFD and publicly available information about past failures in critical infrastructures.

This research makes at least two contributions to practitioners. First, the research helps young engineers have a broader view of security concerns when designing systems that are prone to cyber attacks. Young engineers can use the resource knowledge inventory rather than rely on just their knowledge gained from education and personal experiences. Since "the human" is still recognized as the weakest link in a security chain (Katz et al., 2016), the use of a resource knowledge inventory will enhance their understanding of potential failures in systems and may help them to take proactive actions to mitigate risks of cyber failures.

The second contribution this research makes to practitioners is that it demonstrates how to use a resource knowledge inventory to predict failure scenarios of a specific target system.

1.7 Organization

Chapter 2 provides a review of the literature. Chapter 3 describes the method used to carry out this research. Chapter 4 outlines the results of the study. Chapter 5 provides a

discussion of the results. Finally, Chapter 6 provides conclusions, identifies the limitations of the research and makes recommendations for future work.

2 Literature review

2.1 Background

Integration of smart devices into the traditional topology of industrial infrastructure has evolved it to relatively smart systems. This, enhanced the quality of monitoring and controlling systems on the one hand and becomes an Achilles' heel of the system from security point of view.

The number of cyber failures in critical infrastructures continues to increase (McAfee, 2015). Potential catastrophic consequences from these failures is a major concern (Katz et al., 2016; Wang & Lu, 2013; Kalogridis et al., 2014; Tweed, 2014; Zio, 2016 a, b). The United States has considered this paramount by issuing versions of North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) regulations. The National Institute for Standards and Technology (NIST) framework for protection of critical infrastructure cybersecurity, Canada's Action Plan for Critical Infrastructure, and European Critical Infrastructure Warning Information Network are just a few number of several governmental policies to investigate cybersecurity threats to critical infrastructure (Katz et al., 2016).

Installing smart devices without robust security protections resulted in a hybrid structure in current industrial sites and critical infrastructures causing vulnerabilities in Industrial Control Systems (ICS) and cybersecurity challenges such as stealing or injecting data for malicious goals or controlling components by unauthorized access or

even by physical access to remote compartments that were not protected properly (Katz et al., 2016).

Operating system of embedded computing devices have less protection than server-level computers due to lack of proper software stacks, logging, and audit in TCP/IP (Transmission Control Protocol/ Internet Protocol). These components are used in several smart devices such as smart meters, relays, and substation control systems but simplified in order to limiting hardware requirement or reliability. Recently, cybersecurity policy makers enforce development of protection guards for these devices by protocols and regulations (Katz et al., 2016).

2.2 Failure anticipation in critical infrastructure

Industrial systems are vulnerable to cyber breach by 96 percent in average. Continuously new attackers with new skill sets are joining to the battle to find a vulnerability to cause a cyber failure. Dark webs were developed for sharing the knowledge and complementing professional attackers. On the other hand, stakeholders of critical infrastructures need to secure the systems, operations, human interactions and dynamic information management. This warfare requires anticipating strategies to take first move advantage (Rawal et al.,2016).

Although future failures anticipation is challenging for stakeholders of complex systems, some information about potential failures in a system can improve decision making in present. Attack graph is the most common method of risk analysis and failure

prediction, while it only provides static information about potential failure (GhasemiGol et al.,2016).

Traditional failure analysis methods such as HAZOP, HazID, fault tree, and event tree analysis are investigating the systems to find what can go wrong. While, these methods are based on linear inductive thinking and are not able address topological, behavioral, and dynamic aspects of systems. Increasing number of "surprise events" indicates that different perspectives than traditional ways are required to investigate potential failures in systems (Zio, 2016 a).

Other techniques such as Red Team analysis techniques and penetration test are being used to discover vulnerabilities of a system under study by asking attackers to break into system under controlled condition (Loewengart, 2012). While, Red Team Journal in several articles indicated that the outcome of this attack maneuver significantly depends on the *quality and experience of red team*, *the team's approach and toolset*, and *the overall context of attempt.* It is stated that culturally biased and overconfident team will not help the systems' security.

Statistics shows that system-level breakdowns were initially caused by small distresses with cascading consequences. Predicting cyber failures in complex systems encounters barriers to address behavioral, functional, topological and human interaction vulnerabilities (Zio, 2016), while human is stated to be the most vulnerable factor in

cybersecurity that need impact measurement, security programs, training, and authority limitations (Katz et al., 2016).

Recently, different scholars suggested to use Anticipatory Failure Determination (AFD) method for proactive cybersecurity in the systems (Boyes, 2013; Clothier and Walker, 2015; Gay and Sinha, 2012; Masys, 2012; Zio, 2016 a, b). Application of AFD has been studied during this research to find factors that enable and constrain the use AFD in cyber domain.

2.3 Anticipation theory

Robert Rosen (1985) defines anticipatory system as "A system that contains a predictive model of itself and/or its environment, which allows it to change state at an instant in accord with the model's predictions pertaining to a latter instant".

If we consider system S, as interest system, and model it in M in such a way that S is parametrized in real-time and M parametrized by time variable which is quicker than real-time. We can predict behavior of S from behavior of M at specific time t. Interaction between M and S through a set of effector E , which change the dynamical properties of S and enables M to influence S directly or by changing environmental inputs.

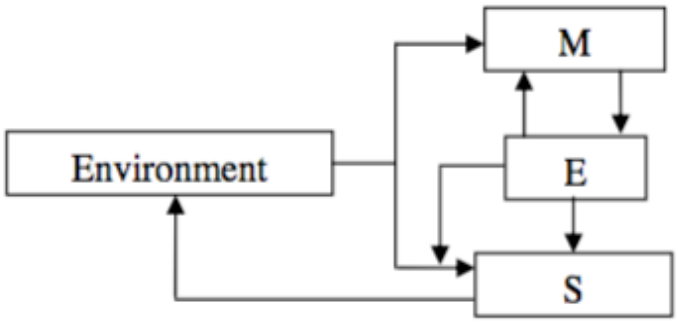

Figure 1- Rosen's definition of Anticipatory system

Anticipatory system according to Rosen's approach is adaptive system which defines current state based on predictions about future (Kohout, 2011).

2.4 Anticipatory failure determination method

Anticipatory Failure Determination (AFD) introduced by Kaplan et al. (1999) is an application of an advance form of Russian-developed Theory of Inventive Problem Solving (I-TRIZ) namely *Scenario Structuring* which is a subset of Risk Analysis AFD is based on principles that employ traditional RA methods to develop future failure scenarios that called Theory of Scenario Structuring.

The AFD method accumulates and organizes the worldwide experience in the operation and design of various systems, to make this knowledge available to new designers, in such a way that the mistakes, accidents and oversights of the past, provide insight for engineering activities and culture in future (Kaplan et al., 1999).

Kaplan et al. (1999), Proseanic et al. (2000), Sunday (2014), and Regazzoni and Russo (2010) are the literatures that used AFD method to solve problems in manufacturing and process development while to the knowledge of this research no literature has used the AFD to predict cyber failures using publicly available information about the past cyber failures in critical infrastructure.

To develop scenarios, the principles defined by Kaplan et al. (1999) as follows:

2.4.1 Principles of scenario structuring

1) The principle of S0

S0 is the "success" scenario or "as-planned" scenario which clearly defines what that system or activity designed for.

2) The principle of initiation (Si)

A failure scenario from as-planned scenario (S0), must have point of departure-a point at which something causes different consequence from expectations, which called Initiating Failure or Initiating Event (IE).

3) The principle of emanation

Each IE could be initiation of different scenarios depend on latter situations which is the way scenario tree are developed. Each path through the tree represent specific scenario and continues until reaches the "end" of scenario, called end state.

4) The principle of unending cause-effect

Every cause-effect chain is extendable in both directions since each happening has its own consequences and initiations.

5) The principle of subdivision

Every scenario could be extended to different new scenarios in more details.

6) Pinch Point Principle

Scenario tree may have pinch points, independent of upstream path leads to those points. These point are also called middle state. (MS)

7) Fault and event trees

There are variety sets of probable failure scenario for any real-world situation and managing and organizing these scenarios in order to identify most and least critical ones and define priorities is the main challenge.

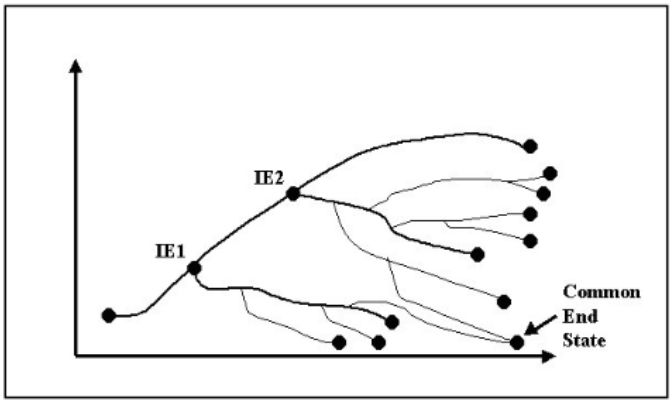

Figure 2-Branches from two different trees can end at the same end state (Kaplan et al.,1999)

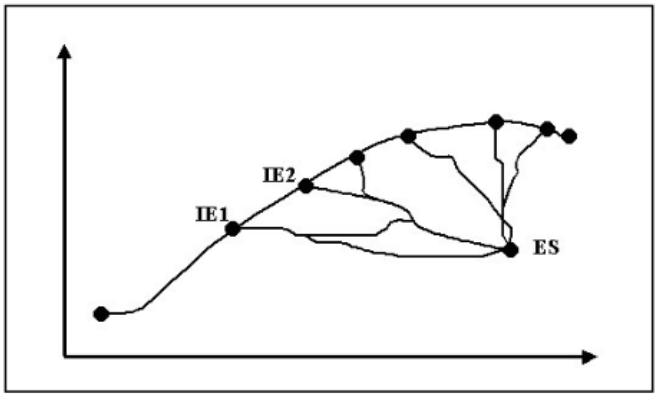

Figure 3-Incoming scenario tree(Kaplan et al.,1999)

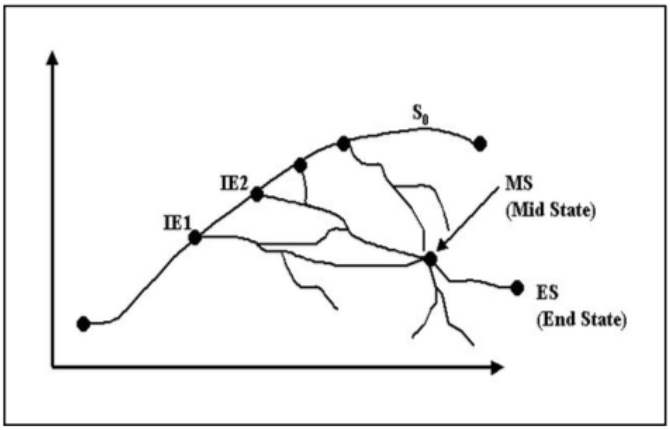

Figure 4-"mixed" Scenario tree(Kaplan et al.,1999)

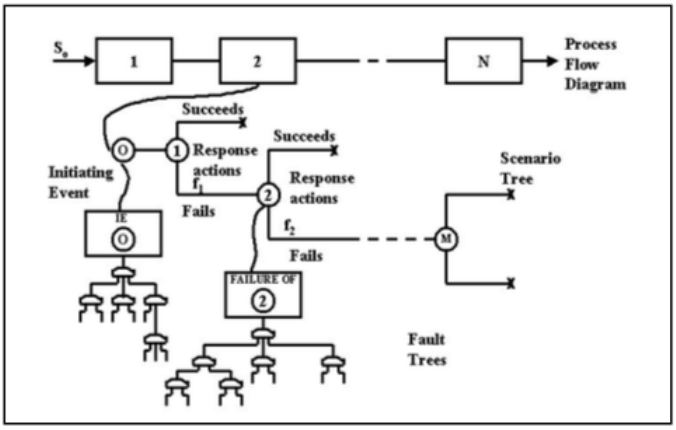

Figure 5- Combined Use of Forward and Backward Trees(Kaplan et al.,1999)

8) The principle of resources

All the configurations, time, space, fields and other factors engaged in specific event are called *resources*. Based on this definition all of the resources should be available in order to have that event been happened and without even one of the resources the failure will not happen.

2.4.2 Scenario structuring using fault and event trees

Scenario Structuring suggested by Kaplan et al. (1999) develops event trees in three ways:

1) Find the possible IEs and draw the outgoing trees from each
2) Find the important ESs and draw the incoming trees to each
3) Find important mid-states and draw the incoming /outgoing trees to each

2.4.3 AFD Applications: Failure Analysis (AFD-1) and Failure Prediction (AFD-2)

Differentiation of AFD with other methods of failure anticipation is to invent failures by changing attitude toward failure. Instead of learning from past failures to prevent them in future, AFD looks for failures that has not happened before. Indeed, instead of asking "What can go wrong in my system?" AFD asks "How can I make things go wrong in the most effective way?" as well as asking "How can I create the particular (proposed) failure?". Once the failure methods identified they can be prevented or limited. All the required conditions and criteria for failure occurrence called resources.

AFD is constitute of two processes of Failure Analysis (AFD-1) and Failure Prediction (AFD-2). AFD-1 finds the roots of the failure that has already happened using RA methods mentioned in 2.2. AFD-2 predicts all the possibilities to predicts new failures using knowledge inventory accumulated from several AFD-1 cycles. AFD-2 application will result in creative solutions to cause failure and predict scenarios that have not happened before.

2.4.3.1 AFD-1: Failure Analysis

The structure of "thought process" in AFD-1 is stated as:

Step 1: Formulate the original problem including naming the system, its purpose and failure situation

Step 2: Identify the success scenario: phases of operation, intended results in each phase

Step 3: Localize the failure to reduce the area of analyze by identifying the last event that during which or right after which the failure happened.

Step 4: Formulate and amplify the inverted problem by changing the attitude to create observed failure.

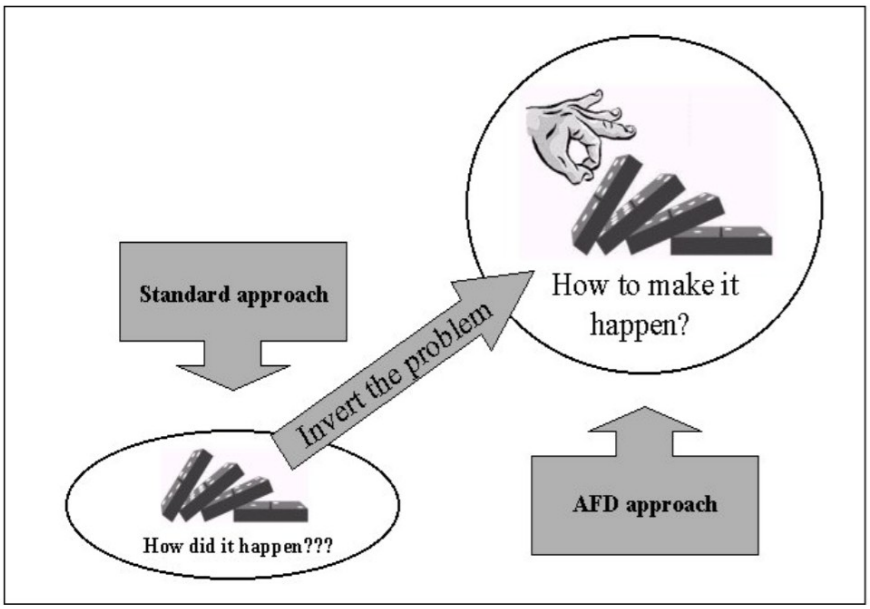

Figure 6- Inverting the Problem(Kaplan et al., 1999)

Step 5: Search for solutions to cause identified failure. This is the area that research, patents, and experience come to practice to search for standard and obvious solutions, identifying resources such as required substances, fields, spaces, time, information, functions.

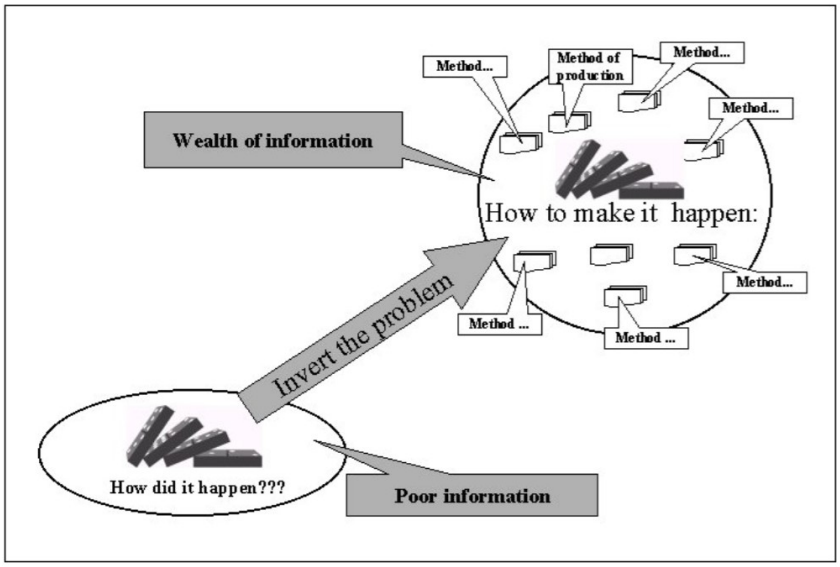

Figure 7- Inverting problem from "How does it happen?" to " How can it be produced?" (Kaplan et al., 1999)

Step 6: Formulate hypotheses and design test to verify them by comparing "what is needed "to create specific failure, and "what exist" leads us to develop different hypotheses.

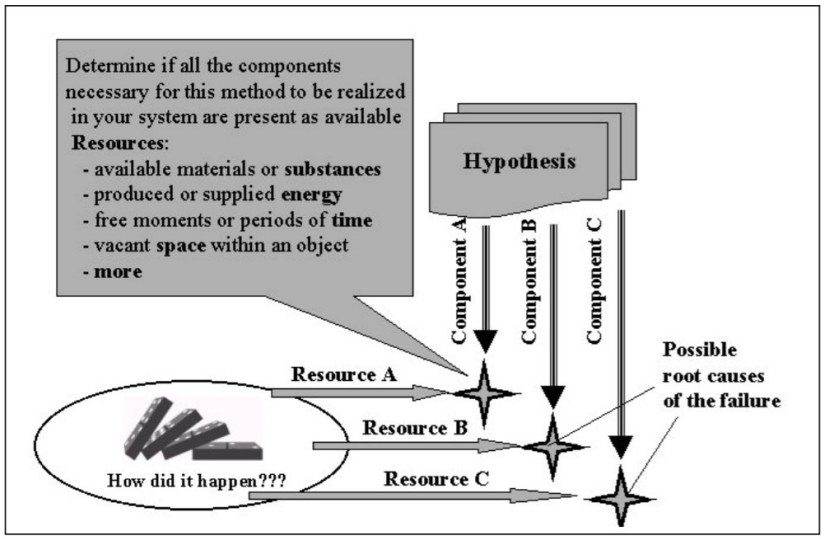

Figure 8- Utilization of resources(Kaplan et al., 1999)

Step 7: Correct the failure which is the last step to find preventive ways of failures.

Templates to develop AFD-1 retrieved from Kaplan et al. (1999) included in Appendix A.

2.4.3.2 AFD-2: Failure prediction

Failure prediction process is very similar to failure analysis; the only difference is that failure prediction looks for "all" or at least "all of the important " failures that can happen to system which results in IEs, MSs, HESs , and S_is.

Step 1: Formulation of all (or all the important) possible failures

Step 2: Defining success scenario, S_0, phases of process ,and results in each phase.

Step 3: Formulate the inverted problems

Step 4: Find all possible failures of a system by considering IEs, HESs, and MSs individually, then, developing integrated scenario tree by combining them.

Step 5: Survey to find available resources which may cause failures in our system, while they were not considered before. These potential failure scenarios should be added to integrated tree as well.

Step 6: Utilize accumulated knowledge

Step 7: Invent new solutions

Templates to develop AFD-2 retrieved from Kaplan et al. (1999) included in Appendix B.

2.5 Constructive research

The constructive research is used to find solution such as *processes, practices, tools* or *organizational charts* for *practical problems* by employing academic theoretical perspectives. The research process involves following steps (Lehtiranta, 2015):

1) Selecting a practically relevant problem
2) Obtaining a comprehensive understanding of the study area
3) Designing one or more applicable solutions to the problem
4) Demonstrating the solution's feasibility
5) Linking the results back to the theory and demonstrating their practical contribution
6) Examining the generalizability of the results

The examples of constructive research approaches are Chen (2002), Pellerin (2003), and Bhuiyan et al. (2004). In this research A process developed to solve the problem of predicting future cyber failures using publicly available information.

2.5.1 Theory building assessment

Arend et al. (2015) proposed an inclusive theory-assessment framework based on outstanding works of past scholars (i.e. Bacharach, 1989; Boxenbaum and Rouleau, 2011; Dubin, 1969; Eisenhardt, 1989; Gioia and Pitre, 1990; McKelvey, 1997; Mohr, 1982; Priem and Butler, 2001; Suddaby, 2010; Sutton and Staw, 1995; Thomas and Tymon, 1982; Whetten, 1989). It defined the applicable criteria objectively in the form of a table. The application of the table evaluates the theory and leads to possible future development to enhance the theory building (Arend et al., 2015).

Three stages of assessment include assessing 1) Experience: capture the focal phenomenon both academically and practically, 2) Explain: build theory that describes mechanics, 3) Establish: Empirically and critically, diffusion, value in the field. Table 1 demonstrates theory-building criteria and assessment developed by Arend et al. (2015)

Stage	Criteria	Recommendations
Experience	Build on existing theory	Reference to existing work
	Build on valid observations	Number of observations, observers' expertise
Explain	Units: comprehensive, parsimonious	Units are well defined
	Clear laws for units' interactions	Directionality, relationships
	Precise boundary laws	Specify focal dependent variables, sequences, outcomes, etc.
	System state exists	At least one state
	Propositions consistent with model	All three types: fact, value, and policy
	Reasonable assumptions	Clarify flows, bounded rationality
	Logical: explicit causality, no tautologies	Explain causality for main laws; delineate what is not true, split if not coherent
	Coherent	Fit among ontology, epistemology, methodology, human nature assumptions
Establish	Empirically testable	Falsifiable predictions are provide
	Diffused in literature	Number of people engaged is large
	Practitioners value: understandable, nonobvious, and implementable	Ideas written in straightforward way; concepts are field ready; constraints are absorbed into process in the field

Table 1- Theory-building criteria and assessment developed by Arend et al. (2015)

2.6 Resources and resource classification

Literature review demonstrates different criteria to define resources. Kaplan et al. (1999) defined resources the all configurations, substances, time, space, fields, information, functions and other factors engaged in specific event. Christensen and Kaufman (2006) defined resources as people, equipment, technology, product, brands, information, cash and relationships with suppliers, distributors, and customers.

> *Resources are things that can be hired and fired, bought and sold, depreciated or built. Most resources are visible and often are measurable, so managers can know what they have. Resources tend to be*

> *flexible as well: most can be transported across organizational boundaries. An engineer who is a valuable contributor in a large firm can quickly become a valuable contributor in a start-up. Technology developed for telecommunications can be valuable in health care. (Christensen and Kaufman, 2006)*

Langley et al. (2013) suggested to address the ontology of resources in process research, while, different ontologies are defined for resources in the cyber world. Van Heerden et al. (2012) defined the ontology of resources as: Actors, actor location, aggressor, attack goal, attack goal, attack mechanism, automation level, effects, motivations, phases, scopes, targets, vulnerabilities. Syed et al. (2016) defined a unified cybersecurity ontology (UCO) the means, consequences, attack, attacker, attack pattern, exploit, exploit target, and indicators. Undercoffer et al. (2004) defined an ontology for computer attacks which includes target, attack strategy, attacker location and end results (Van Heerden et al., 2012).

Van Heerden et al. (2012) stated that high-quality taxonomy is required to be acceptable, comprehensive, complete, determined, excusive, repeatable, constant and solidly defined, unambiguous and useful (Hansman, 2003). The taxonomy provided by Van Heerden et al. (2012) mainly complies usefulness, mutual exclusivity, comprehensibility and unambiguity, while it is emphasized that broad scope of network attack confines adherence to other requirements (Van Heerden et al., 2012).

Van Heerden et al. (2012) provided subdivision for different classes of taxonomy based on comprehensive literature review to define a basis for ontology as follows:

1) *Actor: Commercial competitor, hacker, insider, organized criminal group, protest group*

2) *Actor location: Foreign actor location, local actor location, intermediate actor location*

3) *Aggressor: Individual, commercial, state, group*

4) *Attack goal: Change data, destroy data, disrupt data, steal data, springboard for other attack goals*

5) *Attack mechanism: Access: brute force, buffer overflow, spear phishing, physical; data manipulation: network-based (i.e. denial of service); Virus-based; Trojan, virus, worm; web application-base: SQL injection, cross-site scripting (XSS); information gathering: scanning, physical*

6) *Automation level: Manual, automatic, semi-automatic*

7) *Effects: Null, minor damage, major damage, catastrophic*

8) *Motivation: Financial, fun, ethical, criminal*

9) *Phase: Target identification, reconnaissance, attack phase: ramp-up, damage, residue; post-attack reconnaissance*

10) *Scope: Corporate network, government network, private network*

11) *Target: Personal computers, network infrastructure device, server*

12) *Vulnerability: Configurations: Access rights, default setup; design: open access, protocol error; implementation: buffer overflow, race condition, SQL injection, variable type checking*

Noy and McGuinness (2001) expressed ontology "a common vocabulary for researchers who need to share information in a domain "while due to newness of the domain and the broad applications still solid ontology has not been accepted to share the information of the cyber domain.

3 Method

Chapter 3 describes the method used to carry out the research. Section 3.1 describes the motivation, research question, objectives, and the approach used to carry out the research. Section 3.2 describes the research method and Section 3.3 provides the summary of this chapter.

3.1 Motivation, research question, objectives, and the approach

3.1.1 Motivation

The primary motivation of this study is to identify the enablers and constraints to use AFD method to predict failures using publicly available information of past failures in critical infrastructure.

3.1.2 Research question and objectives

The research question of this thesis is "how to use publicly available information about past failures in critical infrastructures to predict cyber failures of technology startups?"

The objectives of this research are:

1) Identify the components of the AFD method that can be used to predict cyber failures using publicly available information
2) Develop an anticipatory process to predict failures of non-critical infrastructure systems using publicly available information about past cyber failures in critical infrastructures

3) Predict cyber failures in a target system of a technology startup using the anticipatory process developed

3.1.3 Approach

This research used the constructive approach (Lehtiranta et al., 2015) similar to the research that were done by Chen (2002), Pellerin (2003), and Bhuiyan et al. (2004). First, the drafts of the process and the resources knowledge inventory were developed as prototypes. Then, the drafts were reviewed by three experts (Arend et al., 2015). The feedbacks from the experts were incorporated in final version of the process and the resource knowledge inventory. Final versions of prototypes were used in a sample system in latter stages.

3.2 Research method

Table 2 identifies the steps carried out in this research.

Step	Activity	Outcome
1	Literature review in five streams including cyberattacks anticipation in critical infrastructure, failure analysis methods, anticipation, constructive approach, and classification in cybersecurity	Knowledge gap and set of lessons learned
2	Define the process to transform publicly available information about cyber failures in critical infrastructures into predictions of future failures	A process that uses an anticipatory method and publicly available information to predict failures
3	Produce descriptions of past cyber failures using publicly available information	Descriptions of cyber failures
4	Develop a draft of a resource knowledge inventory using the process developed in step 2 to examine the descriptions of the cyber failures produced in step 3	Draft of a resources knowledge inventory - an inventory of resources that indicated or contributed to past cyber failures in critical infrastructures
5	Incorporate feedback about the process used to examine descriptions of cyber failures and the resource knowledge inventory produced from three experts	Revised process and revised resource knowledge inventory using experts' feedback
6	Use the revised version of the process produced to predict potential failure scenarios in a system	Potential resources that may cause failure, and failure scenarios
7	Identify the factors that enable and constrain the use of the AFD method to predict cyber failures using publicly available information	Enablers and constraints of using AFD method to predict cyber failures using publicly available information

Table 2-Research Method

3.2.1 Lessons learned and knowledge gap

Literature review initially conducted in two streams of cyberattack anticipation in critical infrastructure and anticipation theory. The combination of key words such as "critical infrastructure", "anticipation" or "anticipatory", "prediction" or "predict", and

"cybersecurity" were searched using Google and Google Scholar tools to find related literature published since 2012. Later, three other literature streams, including failure analysis methods, classification in cybersecurity, and constructive theory, were reviewed due to research requirements.

The increasing number of “surprise events” that negatively affect critical infrastructures indicates the need for anticipatory methods that predict and mitigate potential failures from different perspectives. Anticipatory methods that start from a proposed future failure and use deductive methods to investigate the bugs and interconnections that can lead to the failure in the system, provide insight about failure circumstances (Zio, 2016 a).

The AFD method introduced by Kaplan et al. (1999) anticipates failure scenarios as a “creative act” with a comprehensive detailed plan to identify all the resources that are needed for occurrence of a failure in the system (Zio, 2016 a,b). The strength of AFD is intentionally “inventing” the failure events and scenarios using the knowledge inventory. By asking” If I wanted to create this failure, how could I do it?”.

AFD is comprised of failure analysis (AFD-1) and failure prediction (AFD-2). AFD-1 uses traditional risk analysis methods to identify the resources that enabled failures in the past. AFD-2 uses results of several AFD-1 iterations to find all the possible resources that may lead to a failure in the system to anticipate future failures. AFD-2

invents new failure scenarios from the existing resources in the system and defines what is needed for the specific failure to occur.

The literature includes studies of the application of AFD to protect manufacturing processes (Kaplan et al., 1999; Proseanic et al., 2000; Sunday, 2014; Regazzoni and Russo, 2010). The literature, however, does not include studies that report on the application of AFD to predict cyber failures using publicly available information about resources that contributed to the past cyber failures in critical infrastructure.

A cyber failure is a violation of a cybersecurity policy that may result in not being able to fulfill a success scenario – the results that are intended to be accomplished at a given phase (Kaplan et al., 1999).

Critical infrastructure refers to the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and effective functioning of government" (Public Safety Canada, 2015). Today, critical infrastructure combines the intelligent infrastructure with computerized control systems and it is at the core of energy transmission and distribution networks, the telecommunication networks, the transportation systems, and water and gas distribution systems (Zio, 2016 a, b).

3.2.2 A process that uses anticipatory method and publicly available information about past cyber failures in critical infrastructures

Figure 9 illustrates the steps of AFD-1 and AFD-2 as described in Kaplan et al. (1999). AFD-1 uses traditional risk analysis methods to identify all resources that enabled failures in the past, in such a way that without any of the resources the failure cannot be accomplished. AFD-1 organizes the resources in a systematic inventory of resources to facilitate communication.

At the core of the AFD method is the use of private information from several past system failures to produce a resources knowledge inventory and the use of this inventory to predict system failures for the purpose of proactively mitigating them.

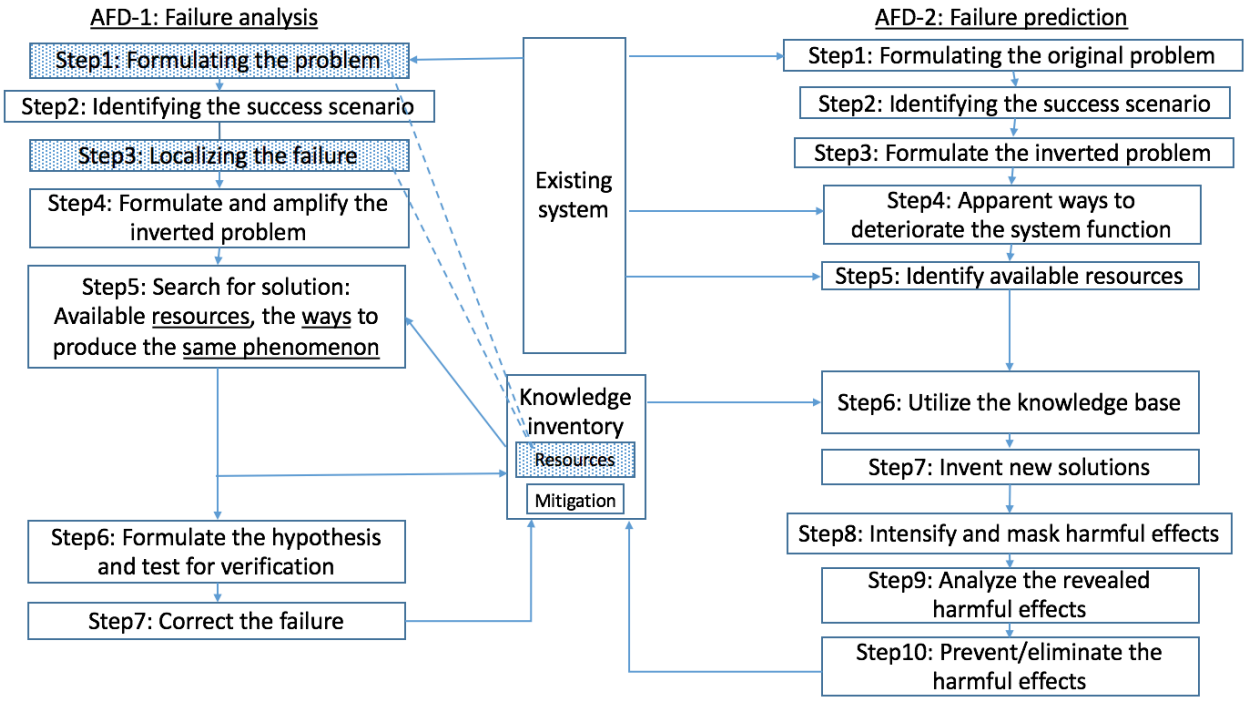

Figure 9-AFD schematic to identify the steps that can be carried out using publicly available information

This research develops a process to transform publicly available information about past cyber failures of critical infrastructure to predict failures of a target system. The process used in this research modifies the elements of AFD-1 and AFD-2 by selecting the steps that can be accomplished using only publicly available information from past cyber failures in critical infrastructures. Since the detail of the systems' design, architecture, and mitigation methods are either confidential or underdevelopment they were not included in the new process.

Figure 10 illustrates the process used in this research to predict failures. This process adapts the failure analysis concept of the AFD-1 and ten cyber failure descriptions extracted from publicly available information to produce a draft of a resource knowledge inventory. The inventory identifies and classifies the resources that contributed or indicated the ten failures. The final version of the resource knowledge inventory can be used to invent potential failures in step 6 of the AFD-2.

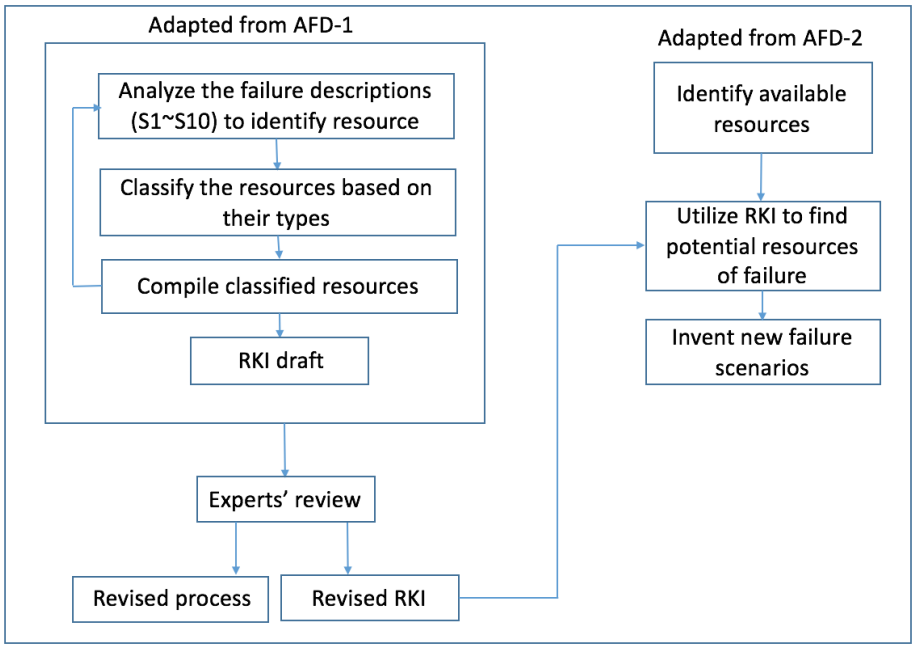

Figure 10-The process used in this research to predict failures

3.2.3 Descriptions of cyber failures

Cyber failures were searched according to following criteria and the selected cyber failures were consulted with a cybersecurity expert to validate the sample.

3.2.3.1 Selection criteria

The selection criteria to develop description for cyber failures in critical infrastructure occurred within last ten years were:

1. Cyber failure in critical infrastructure was an event that English speaking media outlets in North America considered to be newsworthy information
2. Reputable sources provided the information required to describe the cyber failures
3. Five or more resources were identified as being used to cause each cyber failure

4. The supervisor of the thesis deemed the combinations of resources that caused the cyber failures to be of high-diversity

The first criterion required each cyber failure that was included in the sample to meet media outlets criteria for publication according to media college website. The editors of media outlets consider five factors when deciding if a story is newsworthy: timing (e.g., topic is current), significance (e.g., number of people affected is large), proximity (e.g., closeness to home), prominence (e.g., well known organizations and individuals were affected), and human interest (e.g., story appeals to human emotion).

The second criterion required that the sources of information used to describe cyber security failures were reliable. The following sources of information were deemed to be reliable:

1) Articles, books or research papers examined and reviewed by academics
2) Well recognized news organizations such as CNN, BBC, Washington Post, New York Times, Bloomberg, ZDNet, Euractiv.
3) Security reports published by companies that are well-known in cyberspace such as McAfee, Symantec, IBM and Kaspersky
4) Reputable magazines such as Times

The third criterion required that the description included at least five resources about technical details or human errors that indicated or contributed to the cyber-failure. Since the purpose of developing cyber failure descriptions is to produce a resource

knowledge inventory, the cyber failures that have at least five disclosed resources, in publicly available information, were considered in this research.

The fourth criterion required that the sample be of high diversity to enrich the resource knowledge inventory with diverse methods of failure for future applications. Since the resource knowledge inventory will be used as a reference for potential failure resources, the diversity provides broader options to invent failures which eventually can lead to the more robust systems.

3.2.3.2 Search process used to find the cyber failures

The researcher entered various combinations of keywords including "cyberattack", "security breach", "critical infrastructure", "SCADA", “ICS”, “failure” into the Google, Google Scholar search utilities as well as journal databases of Carleton University library to find information on cyber failures published by reliable public sources of information.

The keywords extracted from reliable literatures, were used by Google search engine in several iterations to find more information about the cyber failure. The information about each cyber failure that met all the criteria was included in sample. These descriptions included the hypothesized and simulated failures in ICS (Industrial Control Systems) as well as SCADA (Supervisory Control and Data Acquisition) since they are known academic ways to cause failure, even though they were not representing actual failures in critical infrastructure.

3.2.4 Draft of resource knowledge inventory

Developing resource knowledge inventory helps to identify the combination of resources that frequently contributed to different cyber failures to provides insight about knowing what to expect in the case we identify a resource of failure in our system. Knowing what to expect can increase the potential to identify and mitigate cyber failures.

Comparing the scenarios helped to find similar resources that can be substituted in different systems such as the set of resources contributed to breach the network in different systems. Resource knowledge inventory can be developed further by addition of cross-disciplinary information, such as cyber failures in other domain than critical infrastructures.

Developing a resource knowledge inventory may be a controversial research area in terms of the exposing failure resources to the public and the adverse consequences of training offenders. However, offenders already communicated each other and shared their knowledge through dark web (Weiss and Bailetti, 2015). Resource knowledge inventory is a form of sharing the information about the lessons learned from previous failures to raise awareness and proactively mitigate future cyber failures.

Global contribution to share the experiences and knowledge in a united organized inventory can provide a reference for future junior designers and other stakeholders of systems dealing with security concerns as a heads up about potential failure in their systems.

The descriptions of cyber failures developed in Section 3.2.3 were used to prepare a draft of resource knowledge inventory using the process defined in Section 3.2.2 in following steps:

3.2.4.1 Failure Analysis

The process uses traditional failure analysis methods such as developing scenario trees to identify the resources that indicated or contributed to each cyber failure. To develop a scenario tree, the failure description was reviewed, end-states (ES) or mid-states (MS) were identified. Then, the resources that indicated or contributed to each state were added to the tree. This trend was continued until the initiating states (IS) of the scenario tree were identified. It is likely to be open-ended trend since each state has relevant enabling resources; however, Kaplan et al. (1999) suggested to include at least the most important resources. The outcome of developing scenario trees was identification of the resources that contributed to each cyber failure.

3.2.4.2 Classification of resources

The identified resources were classified to develop an organized draft of resource knowledge inventory. Since the inventory eventually will be used as a reference to predict cyber failures, it needs to have proper order to facilitate retrieving resources.

Literature review demonstrates diverse classifications for resources in the cyber world to address topological, functional, and dynamics of resources that contributed to

the cyber failures (Christensen and Kaufman ,2006; Syed et al., 2016; Van Heerden et al., 2012). To the knowledge of researcher, a comprehensive classification with clear boundaries has not been developed yet and different classifications have been offered for the same or similar set of resources.

In this research, Unified Cybersecurity Ontology (Syed et al., 2016) was chosen to represent the typology of the identified resources. The classes without any matched resources were dismissed from classification of this research (i.e. attacker, exploit). The resources were classified in six typologies of 1) Indicators, 2) Tools, 3) People, 4) Ways, 5) Vulnerabilities, and 6) Information. This classification can be modified for more clarification. Organization of shared information in cyber space to communicate with different disciplines is a new emerging area that needs further investigation and research.

Table 3 provides a succinct definition of six types used to organize the resources that enabled cyber failures. For each resource type, an example is provided.

	Types	Relevant Resource Description	Examples
1	Indicators	Resources that provide evidence of a failure	Destroyed generator
2	Tools	Software and devices used to produce a failure	Port scanner
3	People	Humans that caused the failure to occur	Insider with knowledge
4	Ways	Methods and techniques used to cause the failure	Phishing email
5	Vulnerabilities	Specific element of a system that opens system to attack or damage	Dial-up connection
6	Information	Knowledge or facts learned, especially about a certain subject or event	List of vulnerabilities of a device

Table 3- Classification of resources in cyber failures in critical infrastructure

3.2.4.3 Developing a draft of resource knowledge inventory

The draft of a resource knowledge inventory was developed by compiling the classified resources of the identified cyber failures. The set of organized resources of each scenario represents a row in the table of resource knowledge inventory which the columns signify the classification of resources noted in Section 3.2.4.2. The draft of resource knowledge inventory was completed by positioning all the identified resources of the descriptions in the table. The draft of resource knowledge inventory was finalized after incorporating experts' feedback. The revised version of resource knowledge inventory can be referenced in future predictions.

3.2.5 Revised process and resource knowledge inventory as per experts' review

A review team constitute from three experts that have at least ten years' experience of cybersecurity in the critical infrastructure of Canada in either the public or private sectors. The review session was arranged by the researcher to present the research method and the results to all three experts. It included some time for each reviewer to provide feedback as well as a discussion and brainstorming part for further recommendations to enhance research's productivity by all participants.

Reviewers were asked to evaluate and provide feedback about development and application of process as well as the draft of resource knowledge inventory by providing answers to following questions which are defined according to Arend et al. (2015).

1) How well the proposed process was referenced to the literature of AFD method?
2) How well the proposed process was applied to credible number of cyber failures to extract valid observations?

3) How well the following terms were defined in the research:

- Resources
- Classification and relevant boundaries
- The states of resources including: Indicator, initiating state(IS), mid-state(MS), and end-state (ES)

4) How well the assumption, rationales, and flows were clarified to extract the resources?
5) How well the identified resources were classified in resource knowledge inventory?
6) How well the research is fitting among assumptions in cyber domain in terms of ontology, epistemology, methodology and human nature?
7) How well the process and resource knowledge inventory are empirically testable?
8) How well the process and the resource knowledge inventory are understandable and implementable?

Expert's feedbacks were collected and documented after review session by the researcher to revise the process and the resource knowledge inventory.

3.2.6 Potential resources that may cause failure and failure scenarios

The outcome of the process which is organized in the resource knowledge inventory was tested in a sample system to identify the potential resources that may cause failure and to develop failure scenarios. The sample system is examined to identify the available resources of the system. Different phases of the system during considering, development, operation and maintenance need to be investigated to identify the resource that contributing to the system for comparison with the resource knowledge inventory.

Resources can negatively affect systems either directly such as being used in a system without considering potentiality for corruption or indirectly when similar resources caused cyber failure in another system in the past. The resource knowledge inventory is the reference to identify the resources of the past cyber failures.

In the case matched resources were not found in the resource knowledge inventory the AFD method suggests to investigate each phase of the target system to find what can happen if that phase cannot be completed successfully. Therefore, it starts from a potential failure in each phase of the system and searches for the required resources to cause the failure. If necessary resources to cause failure is missing, it is suggested to create necessary resources from those resources that are available. Combination of invented failures in different phases results in predicted failure scenarios that called scenario structuring (Kaplan et al., 1999).

3.2.7 Enablers and constraints of using AFD method to predict cyber failures using publicly available knowledge

The practical process provided in this research influenced by AFD uses publicly available information to identify the resources, and shares the information in an organized resource knowledge inventory to provide insight and to prevent future failures. During this research the factors that enable or constrain application of the AFD method to use publicly available information to predict cyber failures will be documented.

3.3 Summary

Chapter 3 describes the research method. The main motivation of this study was to identify enablers and constraints to use AFD method to predict failures using publicly available information of past failures in critical infrastructure. The constructive approach was used to define a process to predict potential failures using publicly available information about past cyber failures. The process analyzed cyber failure scenarios, identified and classified resources that contributed to those failures in the past. Resource knowledge inventory was developed by compiling the classified resources of the cyber failures.

4 Results

The purpose of Chapter 4 is to provide the results of applying the process to the identified past cyber failures in critical infrastructures. Section 4.1 identifies the cyber failures examined in this research and their timeline as well as the study period. Section 4.2 describes the process defined to use publicly available information about past cyber failures in critical infrastructures to predict failures. Section 4.3 provides the failure descriptions and classified resource. Section 4.4 provides the resource knowledge inventory. Section 4.5 describes experts' feedback on the process defined in this research and the resource knowledge inventory produced. Section 4.6 provides potential resources that may cause failure and failure scenarios for a sample system. Finally, Section 4.7 provides enablers and constraints of using AFD method to predict failures using publicly available information.

4.1 Sample, timeline and study period

Table 4 demonstrates the ten descriptions of past cyber failures in critical infrastructures identified according to defined criteria for samples. Identified scenarios were consulted with a security expert with 25 years' experience protecting the critical infrastructure of the government of Canada to validate the sample.

	Name of Cyber Failure	Time of failure occurrence	Indicator of cyber failure at the end-state	Reason given for cyber failure
S1	Aurora	March 2007	Power generator destroyed	Unauthorized access to breakers to open and close it quickly
S2	Baku-Tbilisi-Ceyhan (BTC) Pipeline	Aug 2008	Oil pipeline exploded	Command of ICS were manipulated by unauthorized access via the network of surveillance camera to computer network in valve station
S3	Stuxnet	June 2010	About 1000 centrifuges in nuclear infrastructure destroyed	Command of ICS were manipulated by unauthorized access via USB and network's shared points to programming software
S4	RuggedCom	2012	Industrial Control Systems Cyber Emergency Response Team (ICS- CERT) published the threat to critical infrastructures	Backdoor provided unauthorized remote access to communication devices in the critical infrastructure
S5	Flame	May 28, 2012	Kaspersky Lab antivirus discovered a malware in computer system of national oil company	Modular malware is an espionage toolkit that was used to exfiltrate top secret files and send them to external command and control (C&C) servers
S6	German Power Utility (50 Hertz)	Nov 2012	Sustainable power utility went out of service	Distributed Denial of Service (DDoS) attack with a botnet behind it
S7	Aramco	Aug 2012	Information in 35,000 computers of a national oil company was wiped or destroyed	Shamoon malware included modules for self-copying, reporting and wiping data, entered the computer network via a response to a phishing email
S8	German Steel Factory	2013	Blast furnace of a steel mill system could not be shutdown	Commands of ICS were manipulated by an unauthorized access caused by responding to a phishing email
S9	Ukrainian Electrical Grid	Dec 23, 2015	Seven 110 kV and twenty-three 35 kV substations were disconnected from the grid	Commands of ICS were manipulated by an unauthorized access caused by responding to a phishing email
S10	Kingo database	June 2016	Confidential information of 18,800 clients were exposed in a web database	No password or another security protocol was in use to protect data

Table 4- The ten cyber failure in critical infrastructures identified in criteria

Table 4 illustrates the timeline for the ten cyber failure in the sample. The study period is from March 2007 to August 2016.

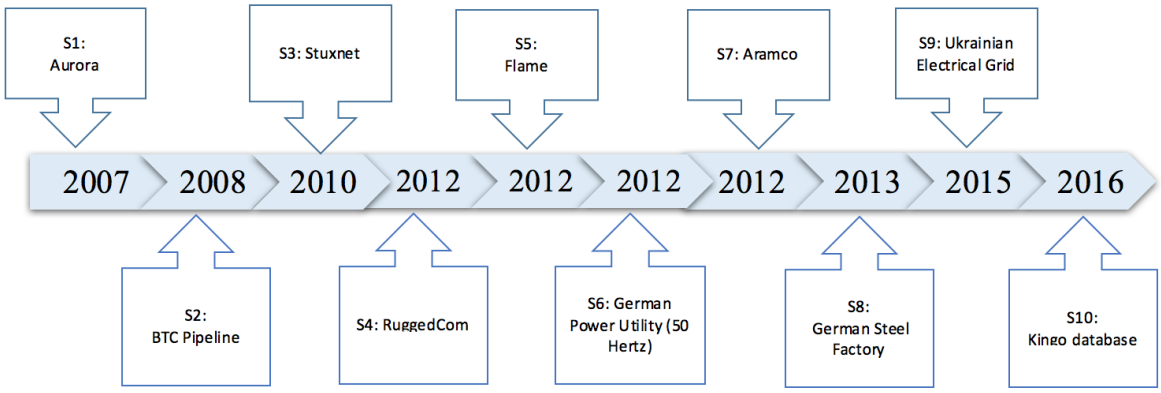

Figure 11- Timeline of past cyber failure in critical infrastructure included in the sample

The names of the cyber failures were chosen based on their labels in the respective literature. Table 5 represents the naming convention for the names of cyber failures.

	Name of the cyber failure	Description
1	Aurora	The name that Idaho National Laboratory chose for the test
2	Baku-Tbilisi-Ceyhan (BTC) Pipeline	The location of the cyber failure
3	Stuxnet	The name of software
4	RuggedCom	The company that produced vulnerable products
5	Flame	The name of software
6	German Power Utility (50 Hertz)	The company that cyber failure took place.
7	Aramco	The company cyber failure took place
8	German Steel Factory	The company cyber failure took place
9	Ukrainian Electrical Grid	The cyber failure location
10	Kingo database	The company cyber failure took place

Table 5- Naming convention

4.2 The Process used publicly available information about past cyber failures in critical infrastructures to predict failures

The process defined in Section 3.2.2 is used to analyze the ten cyber failures listed in Table 4 to identify the resources that indicated or contributed to the ten failures. Scenario trees are developed to analyze each cyber failure and to identify resources. The identified resources were classified according to classification stated in Table 3.

Classified resources of the ten cyber failures were compiled to develop a draft of resource knowledge inventory. The whole process and the draft of resource knowledge inventory were reviewed by cyber experts and feedbacks were incorporated. The revised resource knowledge inventory was used to predict cyber failure in a sample system. The predicted scenarios are the hypotheses for further study and consideration during design or reconfiguration process of systems for proactive mitigation.

4.3 Cyber failure descriptions and resource

For each of the ten past cyber failures in critical infrastructure included in Table 4 , the remainder of this section provides the ten failure descriptions and classified resources extracted from publicly available information in defined criteria. Appendix C includes scenario trees developed for the ten descriptions to analyze the cyber failures and to identify the list of resources contributed to each cyber failure. In failure analysis the relationship between the resources were not addressed in this research and scenario trees were only developed to identify the resources of each state from the literature.

4.3.1 Aurora (2007)

In March 2007, Idaho National Laboratory experimented with a simulated failure in electrical infrastructure that falsified commands from ICS led to physical damage to power infrastructure. In this experiment, rapid open-and-close commands to a breaker connected to a generator in the substation-level, led to smoke emissions from the generator and destroyed it. The failure happened because of "out of synchronism connection of the generator to the grid" (Srivastava et al., 2013). The Aurora cyber failure is among the vulnerabilities of critical infrastructure identified by researchers.

Srivastava et al. (2013) indicated two attack models to damage the generator: local attack (Scenario 1) and remote breaker attack (scenario 2). In Scenario 1, the attack was proposed by inside access to a breaker -or breakers- within a generation level substation; this should have been carried out having insider knowledge and access. In Scenario 2, remote breakers- or a breaker or connected relays to them- were targeted to be opened and closed quickly through manipulated commands. According to Ralethe (2015), old encryption standards made the system vulnerable to data manipulation by unauthorized access.

Vulnerabilities in Ethernet connection and dial up connections enable attackers to breach into the network and make unauthorized access. If the network topology had Ethernet connection, port scanner applications such as Zmap or Masscan could have been used to make unauthorized access to the network. If the network had dial up connection with serial port RS-232 (more vulnerable), MODBUS (Modicon-Bus) address scanner could have been used to make unauthorized access to the network. Having knowledge about finger printing, discovery, access, detection, and connection speed helps offenders

to find a vulnerable relay or breaker in the ICS to manipulate commands (Srivastava et al., 2013).

Table 6 provides the resources drawn from the Aurora description. Resources that led to the failure are organized into six types. The resources shown in Table 6 will be used in the resources knowledge inventory to make predictions in later steps.

	Type	Resources in Scenario 1	Resources in Scenario 2
1	**Indicator**	Generator destroyed	Generator destroyed
2	**Tools**	Breaker or breakers, generator	Breaker or breakers or connected relays to them, generator, port scanner(i.e. Zmap, Masscan) , MODBUS address scanner
3	**People**	Insider with access	
4	**Ways**	Open and close the breaker quickly	Commands to the breakers manipulated via unauthorized access
5	**Vulnerabilities**	Out of synchronism connection of the generator to the grid	Out of synchronism connection of the generator to the grid, old encryption standards, Ethernet and dial-up connection vulnerabilities
6	**Information**	Insider knowledge	Insider knowledge, Knowledge about finger printing, discovery, access, detection, and connection speed

Table 6- Aurora resource types

4.3.2 BTC Pipeline (2008)

Initially, the explosion of the Baku- Tbilisi- Ceyhan (BTC) oil pipeline in 2008 was thought to be the result of a mechanical failure. Western intelligence services, however, found that the explosion was due to a cyberattack (Bloomberg, 2014).

Taking advantage of the vulnerabilities in an IP-based camera and network design, offenders physically accessed camera and surveillance networks and penetrated to the computer network at the valve station and installed controlling software to enable future unauthorized access. They erased approximately sixty hours of pipeline surveillance videos, shut down alarms, cut off communications, jammed the backup satellite, super-pressurizing the pipeline. Eventually, none of the alarms notified the workers of the incident; normal feedback was sent to the control room. Workers discovered the explosion 40 minutes after it occurred when they discovered the flames (Homeland Security News Wire, 2014).

Further investigations found that an infrared camera, working on a different network in the site, had recorded images of two men with laptops near the pipeline a few days before the explosion. The time of the image matched the time of the security breach of the pipeline system (Bloomberg, 2014).

Base on the provided description, resources of the BTC pipeline cyber failure are extracted and categorized in Table 7.

	Types	Resources
1	**Indicator**	Images of two men with laptops near the pipeline captured by an infrared camera from a different network in the site, 60 hours of surveillance videos erased, alarms shut down, communication cut off, backup satellite jammed
2	**Tools**	IP-based Camera
3	People	Two men with laptops near the pipeline station
4	**Ways**	Physical access to camera, software installed for unauthorized access in future, gas pressure increase in small station to explode the pipeline
5	**Vulnerabilities**	Old encryption standards, IP base camera vulnerability, network design vulnerabilities (penetration from surveillance network to ICS network)
6	**Information**	Time of the image in infrared camera matched with time of security breach

Table 7-BTC pipeline resource types

4.3.3 Stuxnet

Stuxnet was malicious software found in the nuclear infrastructures of Iran in 2010, which caused physical damages to approximately 1000 centrifuges by providing unauthorized access and data manipulation in the ICS. Stuxnet was not detectable for several months, and it is believed that- being supported by insider knowledge- the codes were spread in the networks of stakeholders to gather information and find a way to the target (Wangen, 2015).

Stuxnet breached Microsoft Windows vulnerabilities and mined SQL servers to steal the data of the field devices, PLC model numbers, and IP addresses. Then, by identifying the target, Siemens PLC's responsible to control motor frequency converters in centrifuges, Stuxnet systematically searched the network to find them (Combs, 2011).

Stuxnet was connected to command and control (C&C) servers via LAN and network, for updates, uploading and execution codes. Stuxnet spread by self-copying via network shared points, taking advantage of vulnerabilities in Microsoft Windows, using LNK shortcuts of USB sticks, and gaining access to print spoolers of shared printers to gain unauthorized system-level access to lockdown computers used to program Siemens PLCs (Wangen, 2015).

Stuxnet used vulnerabilities in Siemens Step 7 software and manipulated data about motors' speed that caused centrifuges to be destroyed (Combs, 2011). Also, it manipulated data in alarms and control systems so during the failure process, none of the sensors or alarms triggered, and controlling systems were presenting normal readings until centrifuges' abnormality was finally observed in the stations (Kushner, 2013).

Table 8 provides Stuxnet resource types base on provided description.

	Types	**Resources**
1	**Indicator**	Centrifuges' abnormality
2	**Tools**	LNK shortcuts of USB sticks, print spooler of a shared printer , LAN and network, C&C server, SQL server, stakeholders network
3	**People**	Insider with knowledge
4	**Ways**	Self-copying codes to spread via network shared points to make unauthorized access to lockdown computers used to program PLCs, manipulated data in Siemens Step 7 software that changes motors' speed in centrifuges, manipulated data in alarms and control systems
5	**Vulnerabilities**	Microsoft Windows vulnerability, Siemens Step7 software vulnerability, shared point in system (vulnerable topology design), alarm and sensors vulnerability to unauthorized access (vulnerable security system)
6	**Information**	IP and model of PLC responsible to control motor frequency converters in centrifuges

Table 8- Stuxnet resource types

4.3.4 RuggedCom

RuggedCom is a Siemens company that produces network equipment for harsh environments, such as traffic control systems, railroad communication systems, power plants, electrical substations, and military sites, while also producing serial-to-IP conversions in SCADA systems that are supported by MODBUS and DNP3 protocols (ICS-CERT, 2012).

In May 2012, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) web page published an article about the vulnerability of the "weak cryptography for password" which made a default backdoor for unauthorized access in all RuggedCom products manufactured before 2012.

RuggedCom Remote Operating System (ROS) contained an undocumented backdoor account. The username for the account, "factory", cannot be disabled and its password is dynamically generated using the Media Access Control (MAC) address of the devices (ICS-CERT, 2012). This vulnerability can be remotely exploited by discovering the MAC address of the system by the attacker with minimum skills using online scripts (ICS-CERT, 2012; North American Electric Reliability Corporation public disclosure, 2012; Malashenco et al., 2012). Based on the provided description, Table 9 presents RuggedCom resource types.

	Types	Resources
1	**Indicator**	RuggedCom products before 2012
2	**Tools**	
3	**People**	
4	**Ways**	Unauthorized access to RuggedCom devices
5	**Vulnerabilities**	Weak cryptography for password (Backdoor)
6	**Information**	Online scripts, MAC address of devices

Table 9- RuggedCom resource types

4.3.5 Flame

Flame is a cyber worm constitute modules to conduct espionage attacks, discovered in the network of the Iran National Oil Company, by Russia-based antivirus firm Kaspersky Lab, in May 2012. Flame targeted the vulnerabilities in various Microsoft Windows platforms, using multiple propagation and code injection methods, spread over local networks through shared printers and USB sticks by using print spooler and LNK shortcuts respectively. Flame used a fake proxy for Windows Update to bypass all security mechanisms, gained system level access to lockdown computers, and distributed into the network (Bencsáth, et al.,2012; Wangen et al., 2015).

Flame was equipped with modules to take screenshots, was able to switch on microphones and web cameras (if available) to record audio from the Skype conversations and environment, could browse through attached storage devices, and was able to spy through PDF files and AutoCAD files to steal top secret information. It could log keystrokes, extract geolocations from images and perform Bluetooth function to map devices in area, spy the network traffic, and send data via Bluetooth or through the network. Flame has modules to compress, encrypt, and save all stolen information in a database and send it to C&C server regularly in small packages depend on the network

traffic (Bencsáth et al., 2012). Table 10 shows Flame resource types based on the provided description.

	Types	Resources
1	**Indicator**	Russia-based antivirus firm Kaspersky Lab that found the worm
2	**Tools**	Multiple propagation and code injection methods , LNK shortcuts of USB sticks, print spooler of shared printer, modules to take screenshots, modules to record audio from environment by switching on microphone, web camera or from Skype conversation, modules to browse through attached storage devices, modules to spy PDF and AutoCAD files to steal top secret information and extract geolocations from images, modules to log keystrokes, and modules to perform Bluetooth function to map devices in area, modules to compress and encrypt and save data in a database, modules to spy the network traffic and send data to C&C server in small packages via Bluetooth or network, microphone, web camera, monitors, keyboards
3	**People**	
4	**Ways**	Cyber worm that made unauthorized system-level access to lockdown computers, fake proxy for Window update to bypass security mechanism, modules to conduct espionage attacks
5	**Vulnerabilities**	Microsoft Windows vulnerability
6	**Information**	

Table 10- Flame resource types

4.3.6 German Power Utility (50 Hertz)

A German power utility, specializing in sustainable energy, had been under cyber-attack for five days in December 2012. According to EurActiv report, the CEO of 50 Hertz, Boris Schucht, the attack was a DDOS (Distributed Denial of Service) attack to the network with a botnet behind it. It blocked the internet domains for a couple of hours, and all email and connectivity via the internet was disrupted. Although, the email system has recovered in a short time, the whole system was fixed after five days, thankfully none of the electricity supplies were affected by the failure (EurActive, December 10, 2012; 50

hertz annual report, 2012). Table 11 presents German power utility (50 Hertz) resource types according to provided description.

	Types	Resources
1	**Indicator**	Internet domaines' blockage, emails' disruption
2	**Tools**	Botnet
3	**People**	
4	**Ways**	Distributed Denial of Service
5	**Vulnerabilities**	Network
6	**Information**	

Table 11- German power utility (50 Hertz) resource types

4.3.7 Aramco

Saudi Arabian Oil Company "Saudi Aramco" was targeted by a modular malware named Shamoon on August 15, 2012. Employees noticed the incident when files were disappeared and computers were failed. Approximately 30,000 computers were affected in this attack, but industrial control systems were not disturbed since they were working in separate networks (Bronk and Tikk-Ringas, 2013; MoneyCNN 2015).

Still, it is not known how Shamoon first infected the system. Some resources stated that the initial reason was a response to a phishing email. Shamoon is self-copying malware which copies and executes itself using vulnerabilities in network and security mechanisms (Wangen, 2015; Zhioua, 2013).

Shamoon has three basic modules; dropper, reporter, and wiper. The dropper includes codes to make unauthorized access to other components of systems, installs the malware, and drops the modules. The reporter sends the stolen data back to the initial

attacker via typical HTTP GET request. The wiper, focuses on some targeted files with the names of download, document, picture, music, video, and desktop; to copy, rewrite, and delete them. Finally, it executes master boot records to destroy the disk sectors (Zhioua, 2013). Table 12 presents Aramco resource types based on provided description.

	Types	Resources
1	**Indicator**	Disappeared files, fail in 30,000 computers
2	**Tools**	Email contained malicious link to install malware , Shamoon Malware (modular) ; dropper module to install the malware via unauthorized access to other components; reporter module to send data; wiper module to copy, rewrite and delete files ; HTTP Get request; master boot records to destroy the disk sector
3	**People**	Insider who responded to phishing email
4	**Ways**	Codes to make unauthorized access, respond to a phishing email, target files with names of download, document, picture, music, video, desktop
5	**Vulnerabilities**	Network vulnerability, security mechanism vulnerability
6	**Information**	

Table 12-Aramco resource type

4.3.8 German Steel Factory

In 2013, A German steel factory experienced a massive physical damage due to malfunction in some of their industrial control systems. Investigations demonstrated that an insider's response to the phishing email with a compromised PDF file attached caused malicious codes to gain unauthorized access to the corporate network. The codes were self-executed at the time of opening, bypassed security mechanism taking advantage of vulnerabilities, and connected the attacker to the corporate network (Lee et al., 2014).

It is believed that having insider knowledge as well as ICS knowledge, such as using key loggers and network scanners, led attackers to exploit small sets of

workstations. They used vulnerabilities in Active Directory to allow unauthorized access to ICS networks through corporate network. Codes that manipulated data in ICS system, caused breakdowns in ICS that eventually evaded appropriate furnace shutdowns and caused massive physical damage to the system (Lee et al., 2014). Table 13 presents German steel factory resource types based on provided description.

	Types	Resources
1	**Indicator**	Breakdown in ICS system, furnace cannot be shutdown
2	**Tools**	Key logger, network scanner, self-executing codes
3	**People**	Insider who responded to a phishing email
4	**Ways**	Codes to allow unauthorized access to ICS network, codes that manipulated data in ICS , respond to the email contained compromised PDF file attached
5	**Vulnerabilities**	Security mechanism vulnerabilities, Active Directory vulnerabilities caused unauthorized access to ICS network
6	**Information**	ICS knowledge

Table 13- German steel factory resource types

4.3.9 Ukrainian Power Grid

Kyivoblenergo's public announcement in December 2015 indicated a significant cyber failure in the Ukraine power infrastructure which caused the disconnection of seven 110 kV substations and twenty-three 35 kV substations from the grid. Additionally, two other utilities were malfunctioning and a technical problem occurring at their call center, was avoiding contacts of clients during the blackout. Approximately 700, 000 people were suffered from these incidents (Trivellato and Murphy, 2016).

An insider's response to a phishing email with an Excel document attached caused the network to be compromised with the codes allowing unauthorized access. Security mechanism vulnerabilities helped offenders to penetrate from main servers to ICS. Then,

the codes manipulated data in SCADA, using backdoors in SCADA components, to open the breakers. It was believed that in some substations, breakers were opened with direct commands and SCADA systems were not able to re-close them, so the staff manually fixed the problems (Trivellato and Murphy, 2016).

Codes to disable sensors, alarm systems, ICS responses, and restart commands prevented utilities staff from sighting and fixing the problem to delay awareness process at control stations. Meanwhile, a denial of service attack (DOS) happened at their call center for the same purpose. Table 14 presents Ukrainian power grid resource types based on provided description.

	Types	**Resources**
1	**Indicator**	Disconnection of seven 110 kV substations and twenty-three 35 kV substations from the grid and malfunctioning in two utilities, problem in call center
2	**Tools**	BlackEnergy malware campaign, KillDisk malware
3	**People**	Insider who responded to a phishing email
4	**Ways**	Direct commands to breakers, codes to manipulate data in SCADA to open the breakers, DOS attack to call center, delay awareness process at control station, codes to disable ICS response and restart commands to prevent fixing the problem, codes to disable sensors and alarms to prevent staff from sighting the problem, codes to allow unauthorized access to the network, respond to the email contained infected Excel file attached
5	**Vulnerabilities**	Backdoor in SCADA components, security mechanism vulnerabilities(penetration from main server to ICS system)
6	**Information**	

Table 14- Ukrainian power grid resource type

4.3.10 Kingo Database

In June 2016, the MacKeeper security research team found a web database with no password and the security protocol contained 40 gigabytes of confidential information of customers from an energy start-up, Kingo, accessible on the internet (ZDNet, 2016).

Kingo provides prepaid solar power systems to remote area customers in Guatemala and South Africa by collecting a copy of their national card or passport and providing them with prepaid codes for top-ups. Kingo was saving customer's data, detail of contracts, energy usage, support requests, and other data in a cloud service database (Ant). 18,800 customers' full names, addresses, exact GPS locations of homes, occupations, cell phone numbers, unique state identification numbers, genders, marital statuses, nationalities, the birthplaces, and some pictures, finger prints and signatures were among the exposed data (ZDNet, 2016).

Professional search engines such as Shodan.io can easily locate unprotected webcams, systems, and databases to abuse vulnerable data and violate human rights by private surveillance, which are common between drug cartels and extractivists (ZDNet, 2016). Table 15 presents Kingo's database resource types based on provided description.

	Types	**Resources**
1	**Indicator**	MacKeeper security research team

2	**Tools**	Professional search engines such as Shodan.io
3	**People**	Energy start-up customers
4	**Ways**	Human rights violation (murder or private surveillance)
5	**Vulnerabilities**	Unprotected database saved on the cloud
6	**Information**	Confidential data (18,800 customers' full name, address, exact GPS location of home, occupation, cell phone number, unique state identification number, sex, marital status, nationality, the birthplace, and some pictures, finger prints and signatures)

Table 15- Kingo database resource type

4.4 Draft of resource knowledge inventory

The outcomes of Section 4.3 including classified resources of the ten cyber failures in critical infrastructures, were compiled to develop a draft of resource knowledge inventory.

Table 16 demonstrates the draft of resource knowledge inventor

	Indicator	Tool	People	Way	Vulnerability	Information
Aurora-S1	Generator destroyed	Breaker or breakers, generator	Insider with access	Open and close the breaker quickly	Out of synchronism connection of the generator to the grid	Insider knowledge
Aurora-S2	Generator destroyed	Breaker or breakers or connected relays to them, generator, port scanner(i.e. Zmap, Masscan) , MODBUS address scanner		Commands to the breakers manipulated via unauthorized access	Out of synchronism connection of the generator to the grid, old encryption standards, Ethernet and dial-up connection vulnerabilities	Insider knowledge, Knowledge about finger printing, discovery, access, detection, and connection speed
BTC Pipeline	Images of two men with laptops near the pipeline captured by an infrared camera from a different network in the site, 60 hours of surveillance videos erased, alarms shut down, communication cut off, backup satellite jammed	IP-based Camera	Two men with laptops near the pipeline station	Physical access to camera, software installed for unauthorized access in future, gas pressure increase in small station to explode the pipeline	Old encryption standards, IP base camera vulnerability, network design vulnerabilities (penetration from surveillance network to ICS network)	Time of the image in infrared camera matched with time of security breach
Stuxnet	Centrifuges'	LNK shortcuts of USB	Insider	Self-copying codes	Microsoft Windows	IP and model

	Indicator	Tool	People	Way	Vulnerability	Information
	abnormality	sticks, print spooler of a shared printer	with knowledge	to spread via network shared points to make unauthorized access to lockdown computers used to program PLCs, manipulated data in Siemens Step 7 software that changes motors' speed in centrifuges, manipulated data in alarms and control systems	vulnerability, Siemens Step7 software vulnerability, shared point in system (vulnerable topology design), alarm and sensors vulnerability to unauthorized access (vulnerable security system)	of PLC responsible to control motor frequency converters in centrifuges
RuggedCom	RuggedCom products before 2012			Unauthorized access to RuggedCom devices	Weak cryptography for password (Backdoor)	Online scripts, MAC address of devices
Flame	Russia-based antivirus firm Kaspersky Lab that found the worm	Multiple propagation and code injection methods , LNK shortcuts of USB sticks, print spooler of shared printer, modules to take screenshots, modules to record audio from environment by switching on microphone, web camera or from Skype conversation, modules to browse through attached storage devices, modules to spy PDF and AutoCAD files to steal top secret information and extract geolocations from images,		Cyber worm that made unauthorized system-level access to lockdown computers, fake proxy for Window update to bypass security mechanism, modules to conduct espionage attacks	Microsoft Windows vulnerability	

	Indicator	Tool	People	Way	Vulnerability	Information
		modules to log keystrokes, and modules to perform Bluetooth function to map devices in area, modules to compress and encrypt and save data in a database, modules to spy the network traffic and send data to C&C server in small packages via Bluetooth or network, microphone, web camera, monitors, keyboards				
German Power Utility	Internet domaines' blockage, emails' disruption	Botnet		Distributed Denial of Service	Network	
Aramco	Disappeared files, fail in 30,000 computers	Email contained malicious link to install malware , Shamoon Malware (modular) ; dropper module to install the malware via unauthorized access to other components; reporter module to send data; wiper module to copy, rewrite and delete files ; HTTP Get request; master boot records to destroy the disk sector	Insider who responded to phishing email	Codes to make unauthorized access, respond to a phishing email, target files with names of download, document, picture, music, video, desktop	Network vulnerability, security mechanism vulnerability	
German Steel Factory	Breakdown in ICS system, furnace cannot	Key logger, network scanner, self-executing codes	Insider who responded	Codes to allow unauthorized access to ICS network,	Security mechanism vulnerabilities, Active Directory vulnerabilities	ICS knowledge

	Indicator	Tool	People	Way	Vulnerability	Information
	be shutdown		to a phishing email	codes that manipulated data in ICS , respond to the email contained compromised PDF file attached	caused unauthorized access to ICS network	
Ukrainian Power Grid	Disconnection of seven 110 kV substations and twenty-three 35 kV substations from the grid and malfunctioning in two utilities, problem in call center	BlackEnergy malware campaign, KillDisk malware	Insider who responded to a phishing email	Direct commands to breakers, codes to manipulate data in SCADA to open the breakers, DOS attack to call center, delay awareness process at control station, codes to disable ICS response and restart commands to prevent fixing the problem, codes to disable sensors and alarms to prevent staff from sighting the problem, codes to allow unauthorized access to the network, respond to the email contained infected Excel file attached	Backdoor in SCADA components, security mechanism vulnerabilities(penetration from main server to ICS system)	
Kingo database	MacKeeper security research team	Professional search engines such as Shodan.io	Energy start-up customers	Human rights violation (murder or private surveillance)	Unprotected database saved on the cloud	Confidential data (18,800 customers' full name, address, exact GPS location of home,

	Indicator	Tool	People	Way	Vulnerability	Information
						occupation, cell phone number, unique state identification number, sex, marital status, nationality, the birthplace, and some pictures, finger prints and signatures)

Table 16-Draft of resource knowledge inventory

4.5 Revised process and revised resource knowledge inventory

The feedbacks collected from three experts were incorporated in outcome of the research. The major concern was to clarify definition of resources, and boundaries for classification of the resources. Chapter 2 included the summary of the literature review about the resources however since the classification is still not matured in cyber domain, researcher classified the resources to the closest type based on the description. Future research is required to develop a solid ontology of resources to be used as a common language in the cyber domain.

4.6 Potential resources that may cause failure and failure scenarios for a sample system

The sample system that was investigated in this research was LTW-Start. LTW-Start is a component of the Global Cybersecurity Resource that provides startups with key functionalities to help them globalize early and rapidly and be safer online. The intent is to provide functionality that allow the startup to grow its revenue, value, and importance quickly and through the use of carefully designed operating system, to be safer online. The LTW-Start, tagline is “Start global and safer.”

The general architecture of LTW-Start is shown in Figure 12. The top level tier, tools, provides functions to help the entrepreneurial teams generate cash, manage customer discovery, find trusted suppliers, manage documents, create a website, and have corporate email. The lower tier, setting, refers to capabilities for configuring the “safer”

operating system using ClearOS operating system- a strengthened operating system through minimization of function, addition of security tools, etc.

The plan is to deploy thousands of LTW-Starts around the world and that each LTW-Start would have act as a security sensor reporting to a security operations center.

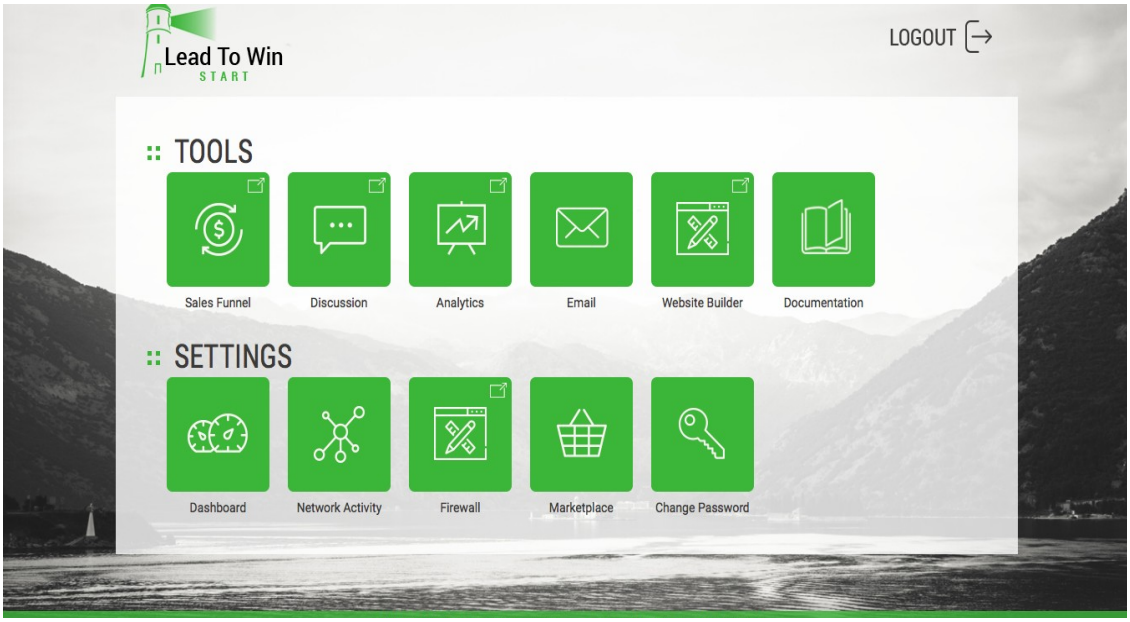

Figure 12- General architecture of LTW-Start

Investigation of the system indicated that the available resources in the system may result in following scenarios in comparison with the resource knowledge inventory. These scenarios are hypothesis for further test and validation while opens a new vision of security concern during developing cycles of the system.

Failure/Indicator: Security operations center receives false network flow information from substantial portion of LTW-Start sensors/installations. Sensor network

is used for spamming campaign. Startup information is stolen.

Tools: Targeted phishing attack through email across sensor network

People:

(i) Targeted phishing campaign increases number of employees of companies who inadvertently succumb to psychological manipulation embedded in phishing email

(ii) Entrepreneurial startup has low cybersecurity talent and varied from expected behavior by reconfiguring underlying ClearOS operating system - unexpectedly turning off various security features

Ways: On clicking phishing email, malicious code is downloaded that immediately surveys OS. Code knows it is ClearOS and explores known vulnerabilities; code tests configuration and finds weak login credentials resulting in full access to ClearOS. Code downloads software to modify security reporting tools (reporting to security operations centre)

Vulnerabilities: Weak credentials, weak configuration allowing downloadable software, 0-day vulnerability in operating systems potentially applicable but weak credentials means it is not needed

Information: Malware steals startup intellectual property

Further concerns were discussed during the investigation session that opened a new perspective to the developer to think of potential failures that can happen in that system.

4.7 Enablers and constraints of using AFD method to predict failures using publicly available information

The enablers to use the AFD method to predict cyber failures were identified as:

1) Frequent contribution of same or similar resources indicates that proper information sharing and preventive methods were not conveyed to all stakeholders and systems were vulnerable to the known failure resources. Resource knowledge inventory can help to distribute the knowledge properly. Specifically, to the junior operation level stakeholders to provide comprehensive knowledge about past cyber failures.

2) Although the AFD method insists on identifying all of the resources of a failure, AFD-2 invents the scenarios from existing resources. It can be concluded that every information about the past failure resources can be used to protect other systems in the case it properly shared to target audience.

3) Collection of the most up-to-date worldwide knowledge about potential failure resources can changes the priorities and enhance the awareness about cyber threats in different systems (Katz et al., 2016).

The constraints to use the AFD method to predict cyber failures were identified as:

1) Although the reports indicated occurrence of hundred thousands of cyber failures around the world (McAfee, 2015), limited number of disclosed cyber failures is the bottleneck of knowledge transmission.

2) Confidential nature of information in cyber domain causes the constraints to extract information about detail of failures, success scenarios, components of systems, and mitigation methods and policies.

3) Different literatures demonstrate diverse descriptions about a same failure. Political perspectives and bias literature were the obstacles to find reliable information.

5 Discussion

Chapter 5 is a discussion of the results provided in Chapter 4. Chapter 5 is organized in six sections. Section 5.1 indicated the challenges of developing the resource knowledge inventory. Section 5.2 discusses process validation. Section 5.3 discusses adaption problem. Section 5.4 discusses using resource knowledge inventory in operation level. Section 5.5 discusses predictions of cyber failure scenarios in a sample system. Finally, Section 5.6 links the results of the research to the reviewed literature.

5.1 Challenges of developing the resource knowledge inventory

Resource knowledge inventory was developed by extracting resources from publicly available information to compose descriptions of cyber failure. Lack of consistent format to describe the cyber failures resulted in diverse style of descriptions provided in Chapter 4. The researcher intended to include all of the resources that were available in public information.

Extracting information to find the failures that disclosed minimum number of resources was challenging due to the lack of inclusive database of cyber failures in public information. This was backing the necessity of developing resource knowledge inventory for stakeholders who desire to learn lessons from cyber failures.

Classification of resources was other challenge because to the knowledge of researcher no dominant ontology has been defined in cybersecurity with clear boundaries

for classification. Different literatures provided different classification for the same set of resources. In this research the closest classification that include most of the identified resources was selected and the classes that were not representing any of the identified resources were not included in resource knowledge inventory.

Classified resources were organized with consideration of the main purpose of developing resource knowledge inventory, its application to predict cyber failures in different systems by stakeholders. Lack of usability rules at this stage makes it challenging to deliver the knowledge with proper application solutions.

5.2 Process validation

Due to the limitations in cyber domain to apply AFD method to predict cyber failures, the new process developed which required to be validated prior to application and test. Expert review incorporated in the process to review the results to avoid bias decision making. Due to immaturity of the domain it was challenging to define how experts can collaborate in validation of the process. A questionnaire developed based on the literature about theory-building assessment to address process validity in a structured format.

5.3 Adoption problem

The review of the resource knowledge inventory indicates that frequent combination of resources have been used in several cyber failures. For instance, emails with malicious link were used in three critical infrastructure cyber failures between 2012

and 2015. Although, these vulnerabilities were known to the stakeholders, the adaption techniques and overall understanding about potential cyber failures in systems were not conveyed properly.

5.4 Using resource knowledge inventory in operation level

Recent controversial discussions and research regarding the significance of sharing information to enhance the overall understanding about potential threats of cyber failure, was practically demonstrated during the research to the researcher. Knowing that many contractors and third parties in small businesses that do not have access and budget to examine reliability of smart devices and their programming, still utilize smart devices in their product without considering the threats being imposed to the end user in critical infrastructure. For example, Aurora is the example of exposing the power grid to a significant failure by using SCADA components that are not well secured.

Developing resource knowledge inventory that organizes worldwide experiences of potential failures can broaden young engineers and designers' viewpoints about security concerns to find potential vulnerabilities of their designs prior to the releasing it to the market as well as restoring critical information of their design and related communication properly. Urging to apply this process autonomously from vulnerability assessment policies at end users' sites will definitely help to protect systems from cyber failures.

5.5 Predictions of cyber failure scenarios in a sample system

Investigation of potential cyber failures in LTW-Start system, showed that developers were more relied on linear failure analysis method rather than thinking to find a way to attack their systems. In some areas quite high-level security plan was considered, while there where some channels without proper security plan that make the whole system vulnerable. Several scenarios defined to cause cyber failure to the system that can be proactively mitigated with no cost.

5.6 Link the results of research to the literature

The review of results demonstrated that all of the ten cyber failure targets were designed and equipped with security mechanisms. Billions of dollars were spent to ensure reliability of the systems; However, all were exploited through the component of the systems and existing vulnerabilities. In some scenarios known vulnerabilities to critical infrastructure stakeholders caused cyber failure again later on (i.e., USB, shared printer). Even though identifying vulnerabilities has prime value, transmitting the knowledge to the wider operation level stakeholders should also be the top priorities.

6 Conclusion, limitations, and suggestions for future research

Chapter 6 is organized into three sections. Section 6.1 provides the conclusions of this research. Section 6.2 identifies the limitations of this research. Section 6.3 provides suggestions for future research.

6.1 Conclusion

The anticipatory process developed and examined in this research to predict future cyber failures in technology startups resulted in developing the resource knowledge inventory as a reference for stakeholders of cyber infrastructures and small technology startups to predict cyber failure scenarios in their systems from a broader view to be mitigated in more cost-effective ways.

The resource knowledge inventory facilitates transmitting information about lessons learned from the past cyber failures in critical infrastructure to be used in non-critical infrastructures and technology startups that may less consider being a target of a cyberattack. The process developed in this research is influenced by the AFD method, while only using publically available information about past cyber failures for scenario structuring. Application of the AFD method to anticipate future cyber failures requires finding the solution, correction and final mitigation method that was not considered in criteria of this research.

Further development of the resource knowledge inventory to include cross-disciplinary knowledge of different cyber infrastructures will enrich the capability to

predict future cyber failures and may provide new solutions for cybersecurity challenges. The worldwide cyber failure experience, as well as academic cyber failure studies, will provide insight to mitigate cyber failures if communicated to the stakeholders of cyber infrastructure properly.

Future cyber failure scenarios are structured based on communicated information between stakeholders.

6.2 Limitations of the research

This research has five major limitations. The first limitation was publicly available information that was narrowed to the results of search tools. However, expanding sources of information to include worldwide experiences from various disciplines will enrich the resource knowledge inventory. Global contribution to building the resource knowledge inventory by crowdsourcing will significantly enhance the efficiency of inventory to anticipate potential cyber failures scenarios.

The second limitation was the lack of solid classification to organize resources due to the immaturity of ontology definition in the cyber domain. A broader research is required to clarify the classification of ontology in cyberspace to facilitate organizing and sharing the information among various disciplines.

The third limitation was the challenge to develop cyber failure descriptions since the information should be formatted to be accessible from the inventory in future to

develop cyber failure scenarios in different systems. The lack of usability guide made the development of failure descriptions and the resource knowledge inventory challenging.

The fourth limitation was the few number of disclosed newsworthy cyber failures in critical infrastructure, which were only ten cyber failures within last ten years, and very few of them have disclosed some details about the cyber failure resources. The small sample size avoided analysis of the results in terms of frequency, trends, and generalization of findings.

The fifth limitation was the practical test of the process. The challenge was extracting all existing resources and details in a sample system including the people, the processes, and all system interactions. Technical startups were not interested in disclosing their information and processes to be studied as a target for potential cyber failures.

6.3 Suggestions for future research

Three areas for future research are suggested in this research. The first suggestion is an open-source platform to engage worldwide stakeholders of cyber systems, to share or use the cross-disciplinary cyber failure experiences, in order to broaden the understanding about potential cyber failures in different systems. Crowdsourcing improves the quality, diversity, scalability of the resource knowledge inventory to communicate the information and to anticipate potential cyber failures more effectively.

The second suggestion is to develop a knowledge inventory of mitigation methods, to include various mitigation methods, their strength, and weaknesses, to help stakeholders of cyber systems gain insight about pros and cons of different mitigation methods to enhance their systems' resilience.

The third suggestion is to execute a broader study to clarify ontology classification for cyber failure resources to facilitate knowledge sharing and cross-disciplinary experience dissemination. The enhanced understanding about potential cyber failure scenarios results in more efficient proactive strategies to improve systems' resilience.

References

50 hertz annual report, 2012. Retrieved from: www.50hertz.com/.../2012%20EN/50Hertz-AnnualReport-2012-en.pdf

Ahmed, A., Kayis, B. and Amornsawadwatana, S., 2007. A review of techniques for risk management in projects. *Benchmarking: An International Journal*, *14*(1), pp.22-36.

Arend, R.J., Sarooghi, H. and Burkemper, A., 2015. Effectuation as ineffectual? Applying the 3E theory-assessment framework to a proposed new theory of entrepreneurship. *Academy of Management Review*, *40*(4), pp.630-651.

Bencsáth, B., Pék, G., Buttyán, L. and Felegyhazi, M., 2012. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet*, *4*(4), pp.971-1003.

Bhuiyan, N., Gerwin, D. and Thomson, V., 2004. Simulation of the new product development process for performance improvement. *Management science*, *50*(12), pp.1690-1703.

https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Boyes, H.A., 2013, October. Trustworthy cyber-physical systems—A review. In *System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International* (pp. 1-8). IET.

Bronk, C. and Tikk-Ringas, E., 2013. The cyber attack on Saudi Aramco. *Survival*, *55*(2), pp.81-96.

Chen, F., 2002. Policies as design and implementation artifacts for non functional requirements.

Christensen, C.M. and Kaufman, S.P., 2006. Assessing your organization's capabilities: Resources, processes and priorities.

Clothier, R.A. and Walker, R.A., 2015. Safety risk management of unmanned aircraft systems. In *Handbook of Unmanned Aerial Vehicles* (pp. 2229-2275). Springer Netherlands.

Combs, M.M., 2011. Impact of the Stuxnet virus on industrial control systems. *XIII International Forum Modern Information Society Formation Problems, Perspectives, Innovation Approaches*, pp.5-10.

Dunjó, J., Fthenakis, V., Vílchez, J.A. and Arnaldos, J., 2010. Hazard and operability (HAZOP) analysis. A literature review. *Journal of hazardous materials*, *173*(1), pp.19-32.

http://www.euractiv.com/section/energy/news/european-renewable-power-grid-rocked-by-cyber-attack/

Gay, L.F. and Sinha, S.K., 2012. Effective Resilience Assessment Methodology for Water Utilities (ERASMUS). *Proceedings of the Water Environment Federation*, *2012*(15), pp.1902-1913.

GhasemiGol, M., Ghaemi-Bafghi, A. and Takabi, H., 2016. A comprehensive approach for network attack forecasting. *Computers & Security*, *58*, pp.83-105.

https://ics-cert.us-cert.gov/advisories/ICSA-13-340-01

https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf

Kalogridis, G., Sooriyabandara, M., Fan, Z. and Mustafa, M.A., 2014. Toward unified security and privacy protection for smart meter networks. *IEEE Systems Journal*, *8*(2), pp.641-654.

Kaplan, S., Zlotin, B., Zusman, A. and Visnepolschi, S., 1999. New tools for failure and risk analysis: An introduction to anticipatory failure determination (AFD) and the theory of scenario structuring. *Ideation International.*

Katz, J.S., Allor, P.G., Dougherty, S.A., Duffy, S.P., Riccetti, S., Chantz, H.D., Kisch, M., Oxford, B.S. and Snowdon, J.L., 2016. Securing the electric power infrastructure. *IBM Journal of Research and Development*, *60*(1), pp.9-1.

Kohout, K., 2011. Multi-level structure of anticipatory behavior in alife.

Kröger, W. and Zio, E., 2011. Vulnerable systems. *Springer Science & Business Media.*

Kushner, D., 2013. The real story of Stuxnet. *ieee Spectrum*, *3*(50), pp.48-53.

Kwon, C. and Hwang, I., 2016. Cyber attack mitigation for cyber–physical systems: hybrid system approach to controller design. *IET Control Theory & Applications*, *10*(7), pp.731-741.

Langley, A., Smallman, C., Tsoukas, H. and Van de Ven, A.H., 2013. Process studies of change in organization and management: unveiling temporality, activity, and flow. *Academy of Management Journal*, *56*(1), pp.1-13.

Lee, R.M., Assante, M.J. and Conway, T., 2014. German Steel Mill Cyber Attack. *Industrial Control Systems*, *30*.

Lehtiranta, L., Junnonen, J.M., Kärnä, S. and Pekuri, L., 2015. The constructive research approach: Problem solving for complex projects. *Designs, methods and practices for research of project management*, p.95.

Loewengart, V., 2012. Anticipating a Catastrophic Cyber Attack.

Malashenko, E., Villarreal, C. and Erickson, J.D., 2012. Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission.

Masys, A.J., 2012. Black swans to grey swans: revealing the uncertainty. *Disaster Prevention and Management: An International Journal*, *21*(3), pp.320-335.

http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

http://www.mediacollege.com/journalism/news/newsworthy.html

money.cnn.com/2015/08/05/technology/aramco-hack/

National Institute of Standards and Technology, 2014. Retrieved from: https://www.nist.gov/cyberframework

National Institute of Standards and Technology, 2016. Retrieved from: https://www.nist.gov/news-events/news/2016/11/new-nist-guide-helps-small-businesses-improve-cybersecurity

North American Electric Reliability Corporation public disclosure, 2012. Retrieved from: http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2012-05-07-01_Ruggedcom_Unauthorized_Access_Vulnerability.pdf

Pellerin, K., 2003. Multimode verification system using fingerprint and speech information.

Proseanic V, Tananko D, Visnepolschi S., 2000. The experience of the Anticipatory Failure Determination (AFD) method applied to an Engine Concern. *TRIZCON2000, May1*.

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

Ralethe, S.G., 2015. Investigating common SCADA security vulnerabilities using penetration testing. *Doctoral dissertation.*

Rawal, B.S., Liang, S., Loukili, A. and Duan, Q., 2016. Anticipatory cyber security research: An ultimate technique for the first-move advantage. *TEM Journal*, *5*(1), pp.3-14.

Regazzoni D., Russo D., 2010. TRIZ Tools to Enhance Risk Management, In Proceedings of the 10th ETRIA World TRIZ Future Conference. *Bergamo, Italia, 3-5 November. ISBN: 978-88- 96333-59-4.*

Rosen, R. 1985. Anticipatory systems. *Philosophical, mathematical and methodological foundations*, New York: Pergamon Press.

Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S. and Adhikari, U., 2013. Modeling cyber-physical vulnerability of the smart grid with incomplete information. *IEEE Transactions on Smart Grid*, *4*(1), pp.235-244.

Sunday, E., 2014. Extension and modification of anticipatory failure determination approach based on I-TRIZ. *Doctoral dissertation, University of Stavanger.*

Syed, Z., Finin, T., Padia, A. and Mathews, L., 2015. Supporting Situationally Aware Cybersecurity Systems.

Teixeira, A., Sou, K.C., Sandberg, H. and Johansson, K.H., 2015. Secure control systems: A quantitative risk management approach. *IEEE Control Systems*, *35*(1), pp.24-45.

Trivellato, D. and Murphy, D., 2016. Lights out! Who's next?.

Tweed, K., 2014. Attack on Nine Substations Could Take Down U.S. *Grid*. Retrieved from: http://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-nine-substations-could-take-down-us-grid.

Van Heerden, R.P., Irwin, B. and Burke, I., 2012, January. Classifying network attack scenarios using an Ontology. *In Proceedings of the 7th International Conference on Information-Warfare & Security (ICIW 2012)* (pp. 311-324).

Wang, W. and Lu, Z., 2013. Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, *57*(5), pp.1344-1371.

Wangen, G., 2015. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, *6*(2), pp.183-211.

Weiss, M. and Bailetti, T., 2015, June. Value of open source projects: A case for open source cybersecurity. In *2015 IEEE International Conference on Engineering, Technology and Innovation/International Technology Management Conference (ICE/ITMC)* (pp. 1-8). IEEE.

http://www.zdnet.com/article/off-the-grid-thousands-exposed-after-database-leak/

Zhioua, S., 2013, July. The Middle East under Malware Attack Dissecting Cyber Weapons. In *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops* (pp. 11-16). IEEE.

Zio, E., 2016 a. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, *152*, pp.137-150.

Zio, E., 2016 b. Critical infrastructures vulnerability and risk analysis. *European Journal for Security Research*, pp.1-18.

Appendices

Appendix A. Template for failure analysis(AFD-1) retrieved from Kaplan et al. (1999)

Step 1. Formulate the original problem

Describe the original situation associated with the undesired phenomenon:

There is a system called {name of the system] for [describe purpose of system]. An undesired effect occurs under the conditions [describe]. It is necessary to find the cause of the phenomenon.

Step 2: Identify the success scenario

Operation or process	Results

Step 3: Localize the failure

Step 4: Formulate and amplify the inverted problem

Step 1. It is necessary to produce [describe inverted problem] under the given condition [describe]

Step 2. It is necessary to produce [describe inverted problem] under the given conditions [describe amplified condition].

Step 5. Search for solutions

The same phenomenon is intentionally created in the following area:

The resources (available or derived) are:

The way(s) to produce the desired phenomenon as found in the innovation Guide are:

ARIZ for failure analysis

Step 1: The general way to produce the desired phenomenon is:

The secondary problem is:

Step 2: The ideal condition for realizing this harmful phenomenon are:

Step 3: The known way to provide the ideal condition is:

The way to change the system, recommended by the Innovation Guide is:

Step4:

A- Limitations to providing the ideal conditions are:

B- Contradiction: There is a way to produce the harmful effect but it cannot be realized for the following reason:

C- According to the Separation Principle, this condition may be resolved in the following way:

Step 6: Formulate Hypothesis and test for verifying them

The hypotheses are:

Tests required to verify the hypotheses:

Step 7: Correct the failure

The way to prevent /eliminate this kind of failure in the future is:

Appendix B. Template for failure prediction (AFD-2) retrieved from Kaplan et al. (1999)

Step 1: Formulate the inverted problem

Describe the original situation associated with the undesired phenomenon:

There is a system called [name of the system] for [describe purpose of the system]. We wish to find all possible undesired effects or failures that can occur within, or as result of, this system, and to identify the ways in which these undesired phenomena can occur.

Step 2: Identify the success scenario

Operations or phases	Results

Step 3: Formulate the inverted problem

There is a system called [name of the system] for [describe]. It is necessary to produce all possible undesired effects or failures that can occur within, or as a result of, this system.

Step 4: Apparent ways to deteriorate the system function

Obvious possible initiating events are:

Obvious harmful end states are:

Obvious possible risk scenarios are:

Step 5: Identify available resources

Substances:

Field resources:

Space resources:

Time resources:

Functional resources:

Systematic resources:

Change resources:

Differential resources:

Inherent resources:

Organizational resources:

Small failures disturbances:

Hazardous elements:

Control devices:

Protection systems:

Step 6: Utilize the knowledge base

Typical weak and dangerous zones in a system:

Typical functional failures:

Typical harmful impacts on systems (humans included):

Typical life cycle stages of technological systems:

Typical dangerous periods in system functioning and evolution:

Typical sources of high danger:

Typical disturbances in flows of substance, energy and information:

Resources:

Step 7. Invent new solutions

The way(s) to produce the harmful effects according to the Innovation Guide are:

ARIZ for failure prediction

Step 1: The general way to produce the desired effect is:

The resulting secondary problem is:

Step 2: The ideal conditions for realizing this harmful effects are:

Step 3: The known way to provide the ideal condition is:

Step 4: The way to change the system, as recommended by the Innovation Guide, is:

A- Limitations to providing the ideal conditions are:

B- Contradiction- There is a way to produce the harmful effect but it cannot be realized for the following reason:

C- According to the Separation Principles, this contradiction may be resolved in the following ways:

Step 8: Intensify and mask harmful effects

Typical ways to intensify harmful effects:

Typical ways to mask harmful effects:

Step 9: Analyze the revealed harmful effects

Step 10: Prevent/eliminate the harmful effects

Typical ways to prevent harmful effects:

Results of working with I-TRIZ operators:

Appendix C

Failure analysis of the past cyber failures conducted by developing scenario trees according to the provided descriptions in Chapter 4, to identify the resources that indicated or contributed to the cyber failures.

Aurora

Figure C. 1 and Table C. 1 respectively providing the failure analysis and identified resources of the Aurora cyber failure.

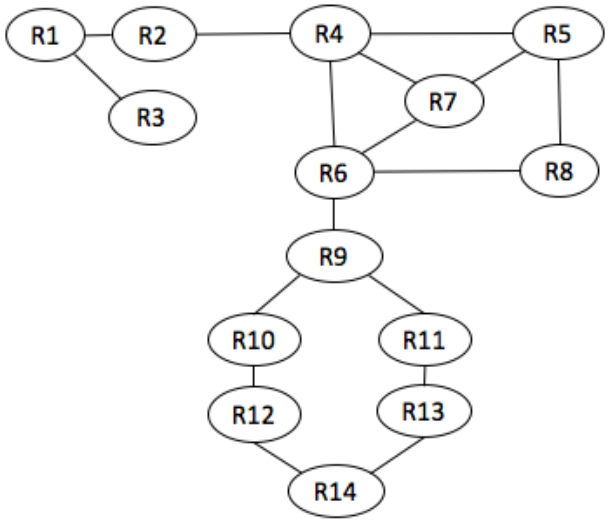

Figure C. 1-Failure analysis (scenario tree) for Aurora cyber failure

Resource No.	Resource Description	Typology
R1	Generator destroyed	Indicator
R2	Out of synchronism connection of the generator to the grid	Vulnerability
R3	Generator	Tool
R4	Open and close breaker quickly	Way
R5	Insider with access	People
R6	Command to the breakers manipulated via unauthorized access	Way
R7	Breaker, or breakers, or connected relays	Tool
R8	Insider knowledge	People
R9	Old encryption standards	Vulnerability
R10	Dial-up connection vulnerabilities	Vulnerability
R11	Ethernet connection vulnerabilities	Vulnerability
R12	MODBUS address scanner	Tool
R13	Port scanner	Tool
R14	Knowledge about finger printing, discovery, access, detection, connection speed	Information

Table C. 1-List of the resource of the Aurora cyber failure identified based on the provided description

BTC-Pipeline

Figure C. 2 and Table C. 2 respectively providing the failure analysis and identified resources of the BTC-Pipeline cyber failure.

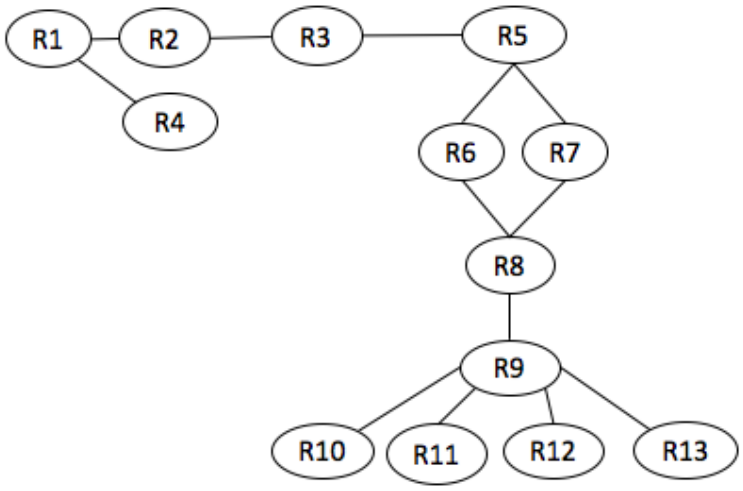

Figure C. 2- Failure analysis (scenario tree) for the BTC-Pipeline cyber failure

Resource No.	Resource Description	Typology
R1	Images of two men with laptops near the pipeline captured by an infrared camera from a different network in the site	Indicator
R2	Two men with laptops near the pipeline station	People
R3	Physical access to camera	Way
R4	Time of the image in infrared camera matched with time of security breach	Information
R5	IP-based Camera	Tool
R6	Network design vulnerability(penetration from surveillance network to ICS network)	Vulnerability
R7	IP base camera vulnerability	Vulnerability
R8	Software Installed for unauthorized access in future	Way
R9	Old encryption standards	Vulnerability
R10	Gas pressure increase in small station to explode the pipeline	Way
R11	60 hours of surveillance videos erased	Indicator
R12	Alarms shut down	Indicator
R13	Communication cut off	Indicator
R14	Backup satellite jammed	Indicator

Table C. 2- List of the resource of the BTC-Pipeline cyber failure identified based on the provided description

Stuxnet

Figure C. 3 and Table C. 3 respectively providing the failure analysis and identified resources of the Stuxnet cyber failure.

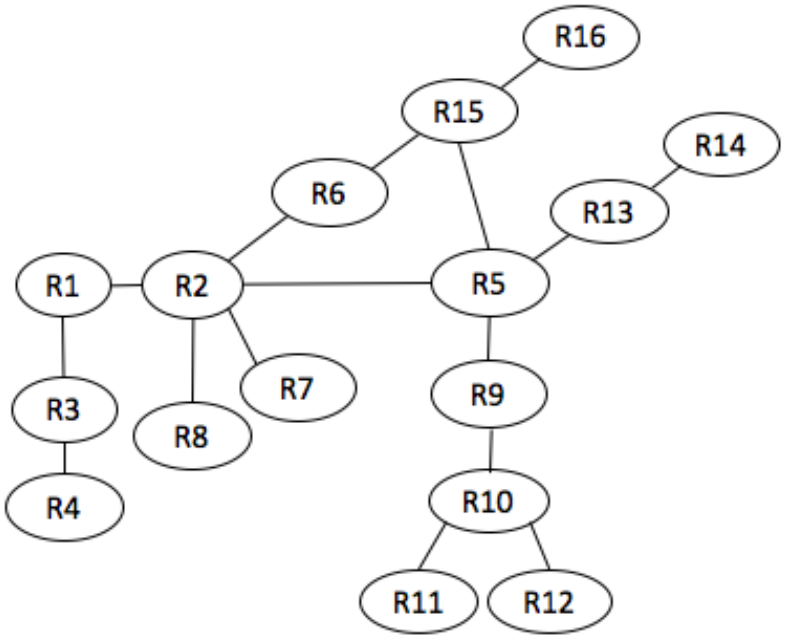

Figure C. 3- Failure analysis (scenario tree) for the Stuxnet cyber failure

Resource	Resource Description	Typology

No.		
R1	Centrifuges' abnormality	Indicator
R2	Manipulated data in Siemens Step 7 software that changed motors' speed in centrifuges	Way
R3	Manipulated data in alarms and control systems	Way
R4	Alarm and sensors vulnerability to unauthorized access (vulnerable security system)	Vulnerability
R5	Microsoft Windows vulnerability	Vulnerability
R6	Command and Control server (C&C)	Tool
R7	Insider with knowledge	People
R8	Siemens Step 7 software vulnerability	Vulnerability
R9	Self-copying codes to spread via network shared points to make unauthorized access to lockdown computers used to program PLCs	Way
R10	Shared point in the system (vulnerable topology design)	Vulnerability
R11	LNK shortcuts of USB sticks	Tool
R12	Print spooler of shared printer	Tool
R13	SQL server	Tool
R14	IP and model of PLC responsible to control motor frequency converters in centrifuges	Information
R15	LAN and network	Tool
R16	Stakeholders network	Tool

Table C. 3- List of the resource of the Stuxnet cyber failure identified based on the provided description

RuggedCom

Figure C. 4 and Table C. 4 respectively providing the failure analysis and identified resources of the RuggedCom cyber failure.

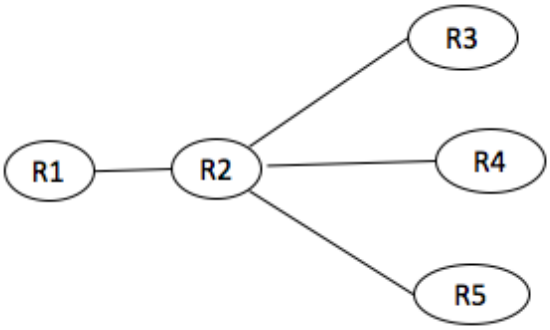

Figure C. 4- Failure analysis (scenario tree) for the RuggedCom cyber failure

Resource No.	Resource Description	Typology
R1	RuggedCom products before 2012	Indicator
R2	Unauthorized access to RuggedCom devices	Way
R3	Weak cryptography for password (Backdoor)	Vulnerability
R4	Online Scripts	Information
R5	Mac address of devices	Information

Table C. 4- List of the resource of the RuggedCom cyber failure identified based on the provided description

Flame

Figure C. 5 and Table C. 5respectively providing the failure analysis and identified resources of the Flame cyber failure.

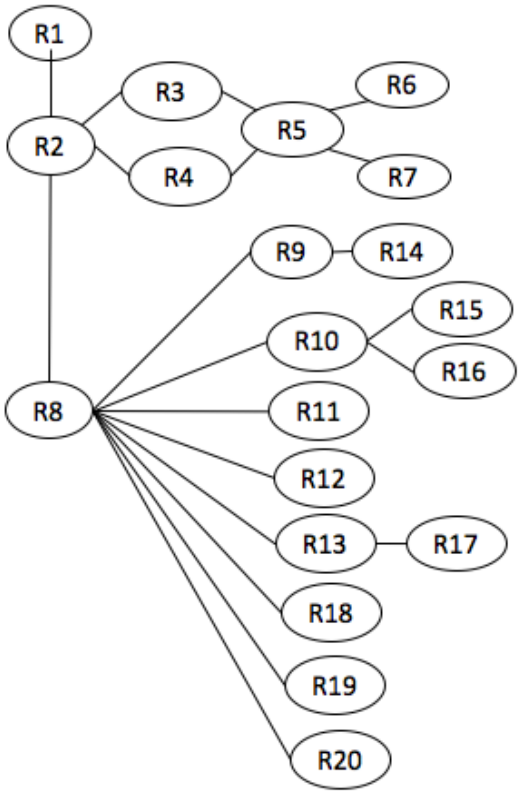

Figure C. 5- Failure analysis (scenario tree) for the Flame cyber failure

Resource No.	Resource Description	Typology
R1	Russia-based antivirus firm Kaspersky Lab that found the worm	Indicator
R2	Cyber worm that made unauthorized system-level access to lockdown computers	Way
R3	Fake proxy for Windows update to bypass security mechanism	Way
R4	Multiple propagation and code injection methods	Tool
R5	Microsoft Windows vulnerability	Vulnerability
R6	LNK shortcuts of USB sticks	Tool
R7	Print spooler of shared printer	Tool
R8	Modules to conduct espionage attacks	Way
R9	Module to take Screenshots	Tool
R10	Modules to record audio from environment by switching on microphone, web camera or from skype conversation	Tool
R11	Modules to browse through attached storage devices	Tool
R12	Modules to spy PDF, AutoCAD files to steal top secret information and extract geolocation from images	Tool
R13	Modules for log keystrokes	Tool
R14	Monitors	Tool
R15	Web camera	Tool
R16	Microphone	Tool
R17	Keyboards	Tool
R18	Modules to compress, encrypt and save information in a database	Tool
R19	Modules to perform Bluetooth function to map devices in area	Tool
R20	Modules to spy the network traffic and send data to C&C server in small packages via Bluetooth or network	Tool

Table C. 5- List of the resource of the Flame cyber failure identified based on the provided description

German Power Utility (50 Hertz)

Figure C. 6 and Table C. 6 respectively providing the failure analysis and identified resources of the German Power Utility (50 Hertz) cyber failure.

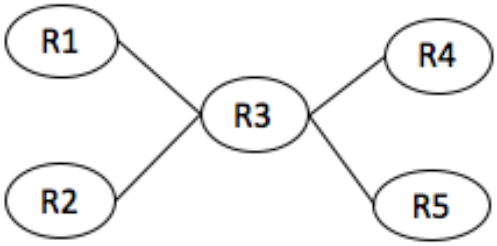

Figure C. 6- Failure analysis (scenario tree) for the German Power Utility (50 Hertz) cyber failure

Resource No.	Resource Description	Typology
R1	Emails' disruption	Indicator
R2	Internet domains' blockage	Indicator
R3	Distributed Denial of Service	Way
R4	Network	Vulnerability
R5	Botnet	Tool

Table C. 6- List of the resource of the German Power Utility (50 Hertz) cyber failure identified based on the provided description

Aramco

Figure C. 7 and Table C. 7 respectively providing the failure analysis and identified resources of the Aramco cyber failure.

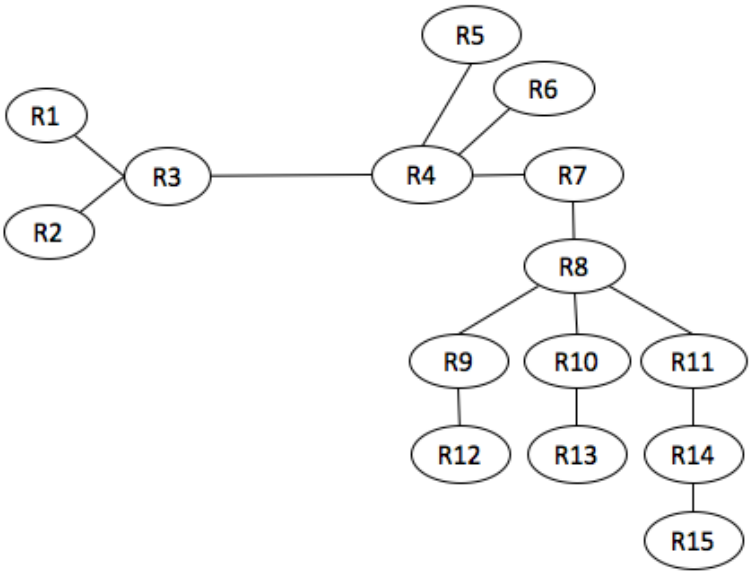

Figure C. 7- Failure analysis (scenario tree) for the Aramco cyber failure

Resource No.	Resource Description	Typology
R1	Disappeared files	Indicator
R2	Fail in 30,000 computers	Indicator
R3	Network vulnerability	Vulnerability
R4	Respond to a phishing email	Way
R5	Email contained malicious link to install malware	Tool
R6	Insider who responded to phishing email	People
R7	Security mechanism vulnerability	Vulnerability
R8	Shamoon malware (modular)	Tool
R9	Dropper module to install the malware via unauthorized access to other components	Tool
R10	Reporter module to send data	Tool
R11	Wiper module to copy, rewrite and delete files	Tool
R12	Codes to make unauthorized access	Way
R13	HTTP Get request	Tool
R14	Target files with names of download, document, picture, music, video, desktop	Way
R15	Master boot records to destroy the disk sector	Tool

Table C. 7- List of the resource of the Aramco cyber failure identified based on the provided description

German Steel Factory

Figure C. 8 and Table C. 8 respectively providing the failure analysis and identified resources of the German Steel Factory cyber failure.

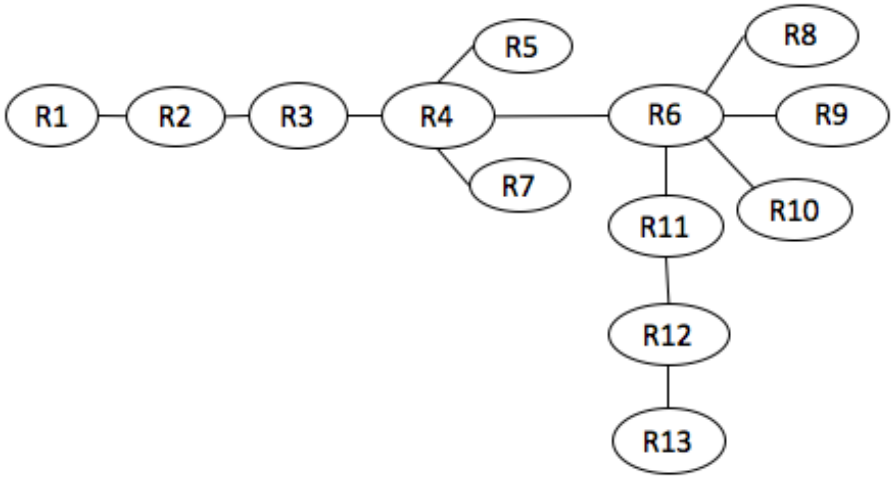

Figure C. 8- Failure analysis (scenario tree) for the German Steel Factory cyber failure

Resource No.	Resource Description	Typology
R1	Furnace cannot be shutdown	Indicator
R2	Breakdown in ICS system function	Indicator
R3	Codes to manipulate data in ICS	Way
R4	Codes to make unauthorized access to ICS network	Way
R5	Vulnerabilities in Active Directory were used to make unauthorized access to ICS network	Vulnerability
R6	Small set of workstations' vulnerabilities	Vulnerability
R7	ICS knowledge	Information
R8	Key logger	Tool
R9	Network scanner	Tool
R10	Self-executing codes	Tool
R11	Vulnerabilities in security mechanism	Vulnerability
R12	Insider who responded to phishing email	People
R13	Respond to the email with a compromised PDF file attached	Way

Table C. 8- List of the resource of the German Steel Factory cyber failure identified based on the provided description

Ukrainian Electrical Grid

Figure C. 9 and Table C. 9 respectively providing the failure analysis and identified resources of the Ukrainian Electrical Grid cyber failure.

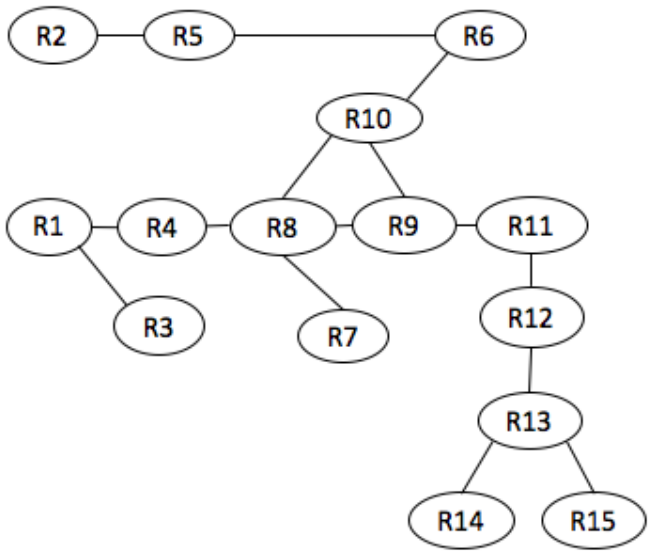

Figure C. 9- Failure analysis (scenario tree) for the Ukrainian Electrical Grid cyber failure

Resource No.	Resource Description	Typology
R1	Disconnection of seven 110 kV substations and twenty-three 35 kV substations from the grid and malfunctioning in two utilities	Indicator
R2	Problem in call center	Indicator
R3	Direct commands to breakers	Way
R4	Codes to manipulate data in SCADA used to open the breakers	Way
R5	DOS attack to call center	Way
R6	Delay awareness process at control station	Way
R7	Codes to disable ICS response and restart commands to prevent fixing the problem	Way
R8	Backdoor in SCADA components	Vulnerability
R9	Security mechanism vulnerabilities (penetration from main server to ICS)	Vulnerability
R10	Codes to disable sensors and alarms to prevent staff from sighting the problem	Way
R11	Codes to allow unauthorized access to the network	Way
R12	Respond to the email contained an Excel file attached	Way
R13	Insider who responded to a phishing email	People
R14	BlackEnergy malware campaign	Tool
R15	KillDisk malware	Tool

Table C. 9- List of the resource of the Ukrainian Electrical Grid cyber failure identified based on the provided description

Kingo Database

Figure C. 10 and Table C. 10 respectively providing the failure analysis and identified resources of Kingo Database Grid cyber failure.

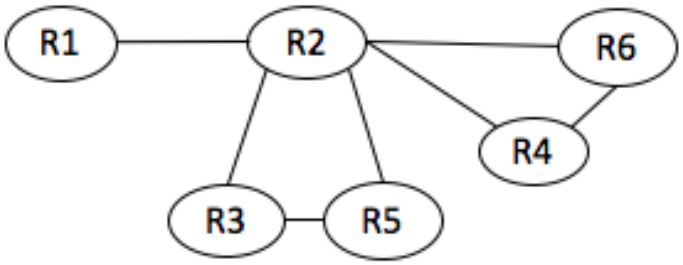

Figure C. 10- Failure analysis (scenario tree) for the Kingo Database cyber failure

Resource No.	Resource Description	Typology
R1	MacKeeper security research team	Indicator
R2	Unprotected database saved on the cloud	Vulnerability
R3	Professional search engines such as Shodan.io	Tool
R4	Energy start-up customers	People
R5	Human rights violation (murder or private surveillance)	Way
R6	Confidential data (18,800 customers' full name, address, exact GPS location of home, occupation, cell phone number, unique state identification number, sex, marital status, nationality, the birthplace, and some pictures, finger prints and signatures)	Information

Table C. 10- List of the resource of the Kingo Database cyber failure identified based on the provided description