University of
Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study programme/ specialisation: M.Sc., Risk Management/Risk Management	Spring semester, 2020 Open
Author: Emmanuel Chukwuebuka Okoli	……………………………… (signature of author)
Supervisor(s): Emmanuel Frederic Bouder	
Title of master's thesis: Risk Governance of a Complex system using Route Redistribution as a Case Study	
Credits (ECTS): 30	
Keywords: Systemic risk and Uncertainty Risk management, Risk Governance Route Redistribution, routing protocols	Number of pages: 65 Stavanger, 15.07.2020

Risk Governance of a Complex System Using Route Redistribution as a Case Study.

Emmanuel Chukwuebuka Okoli

Stavanger, 2020

ABSTRACT

Route redistribution is a communication networking system that allows different routing protocols within a network to communicate with each other. These protocols offer different benefits to the network and network equipment; thus, companies can harness the benefits of the different protocols within their local area network using route redistribution. The benefits offered using route redistribution comes at the cost of systemic risk, which is a risk of breakdown of the entire system.

This Thesis aims to improve the risk governance of the complex system by using the risk governance framework beyond the normal traffic light model to the six-risk classification developed by the German Scientific Advisory Council for Global Environment Change and the use of FRAM and TRAM methods to model uncertainties.

PREFACE

This Master thesis is written as the final part of the MSc in Risk Management at the Faculty of Science and Technology, University of Stavanger, Norway.

Special thanks to my supervisor Frederic Emmanuel Bouder for his relentless guidance throughout this writing. Even when it seemed I did not know what I was doing, he was there to direct my path. I would also like to thank my family and friends for their motivation and support.

Emmanuel Chukwuebuka Okoli

University of Stavanger, Norway, July 2020

TABLE OF CONTENT

List of Abbreviations

ARP	Address Resolution Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FRAM	Functional Resonance Analysis Method
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
OSPF	Open Shortest Part First
RIPv1	Routing Information Protocol version 1
RIPv2	Routing Information Protocol version 2
STAMP	System Theoretic Accident Model and Processes
WAN	Wide Area Network
WGBU	German Scientific Advisory Council for Global Environment Change

List of Figures

List of Tables

Introduction

In a data-driven world of today, the term globalisation cannot be neglected. *"…Globalism is a state of the world involving networks of interdependence at a multicontinental distance…"*(Nye. & Donahue, 2000). It also involves networks of connections, not simply to a single linkage. As we are so dependent on data for our daily activities, there is an increase in network traffic, which poses a risk of frequent failure to the network equipment, especially the routing equipment.

One current example is the COVID-19 pandemic, which resulted in the adoption of work from most companies' home policy. Globalisation changed the transmission of know-how (Archibugi & Pietrobelli, 2003). Globalization has affected systemic risks by increasing the complexity and tight couplings (Renn, Lucas, Haas, & Jaeger, 2019). For example, the 1980 ARPANET collapse, the nationwide saturation of the AT&T routing and switching system in 1990 (Neumann, 1994), the global havoc of the 'iloveyou' virus in the spring of 2000 (Sprinkel, 2001), provides early glimpses of how dependent we have become and the systemic effects of this dependency. According to Nye and Donahue 2000, "*Globalisation will affect governance processes and be affected by them"(Nye. & Donahue, 2000).* This shows that there is a need for twerk in the way we govern and manage those networking devices as they are now prone to experience what may not have been anticipated during the design process of their components.

Many uncertainties surround the nature of today's network traffic, which poses a serious risk of failure in the routing processes. As stated in Nye and Donahue 2000, *"Chaotic Uncertainty is too high for most people to pay for somewhat higher average levels of prosperity. Unless some aspects of globalisation can be effectively governed, it may not be sustainable in its current form"*(Nye. & Donahue, 2000). The amount of information content available online and the endless abilities to communicate globally have prompted users to spend a significant amount of time on the net (Nye. & Donahue, 2000, p. 144). A 1999 study by the Kaiser Family Foundation showed that Internet use might substitute for television viewing among children (Roberts, 1999). Some developing countries have their network servers located and managed in developed countries through cloud computing. All these contribute to a great surge on internal and external (Global) network traffic for companies, thereby creating uncertainties on the reliability of an existing governing framework concerning Networking.

There is a need to lay more emphasis on Systemic Risks, which expands the scope of risk beyond its two classic components; the extent of damage and probability of occurrence to Systemic risk, Uncertainties and Black Swan type of risk in the risk Governance process of a complex system such as Route Redistribution. These lead to the following research questions:

1. Why do we use different routing protocols in a Local Area Network (LAN)?
2. What are the problems associated with route redistribution, and how do they relate to systemic risk?
3. How do we use risk science to improve the management of network routing?

The questions above are developed to better reflect the current risk governance process and practices in handling route redistribution and presenting an improved risk governance framework that emphasizes the treatment of systemic risk, uncertainties, and black swan types of risk.

This Thesis is organised into six chapters; Chapter 1: Literature Review, Chapter 2: Networking Concepts, Chapter 3: Methodology, Chapter 4: Results, Chapter 5: Analysis of Results and Discussion, Chapter 6: Conclusion and Recommendation.

CHAPTER 1

1.1 Literature Review:

A common issue in the field of Networking is on how to deal with an unexpected potential failure of its routing protocols. Within a Local Area Networks (LAN) of a company, the networks are segmented into several other subnetworks to better serve the various departments of the company, and most often, these different departments use different routing protocols (e.g. EIGRP, OSPF, RIPv1, RIPv2). Since these different routing protocols use different communication (i.e. they convey the same message in different languages), in an attempt to globalise the communication between the various protocols, there is a complex system, Route Redistribution serves to communicate the information from one routing protocol to another. Such complex systems are affected by pervasive Uncertainty, which may lead to a surprising effect (Bjerga, Aven, & Zio, 2016). A similar argument can be found in Dirk Helbing 2013, where he said that when networks are interdependent (Global), they are more vulnerable to abrupt failures i.e. hyper-connected networks establish hyper-risks (Helbing, 2013). There is always an intermittent downturn in the network communication today, and this is mostly caused by the systemic effects introduced using route redistribution. Just as Alexander said, "*The solutions to our problem will become a new source of the problem*" (Ač, 2010).

The traditional approach of risk assessment ignores the inherent interactions among risks and fails to cope with ripple effects (M. Fan, Lin, & Sheu, 2008). Peters et al. (2008) claimed that risk interdependence is an important factor for disaster preparedness and anticipative disaster response management (Peters, Buzna, & Helbing, 2008). If risk interdependence can be properly analysed, then substantially effective risk response decisions can be made (Kwan & Leung, 2011). Szymanski et al. (2015) studied the failure dynamics of the global risk network, and the key finding is that risk properties as contagion potential, persistence, roles in cascades of failures and the identity of risks are most detrimental to system stability (Szymanski, Lin, Asztalos, & Sreenivasan, 2015).

Hellstrom 2003, suggests that the key to understanding risk from a perspective of technological innovation then is to understand the infrastructural sphere through which these innovations pervade socio-economic life, which is to understand their critical systemic functions (Hellström, 2003). Route redistribution, which helps to incorporate the benefits of different routing protocols in a Local Area Network, comes at the cost of Contagion risk. The contagion phenomena have been discussed by several authors (Angst, Agarwal, Sambamurthy, & Kelley, 2010; Mann, Kauffman, Han, & Nault, 2011; Slovic, 2013) where the failure of an element within an interconnected network causes the failure of another. This contagion phenomenon is the core aspect of systemic risk.

Systemic risk is defined as a "*crossroad between natural events (partially altered and amplified by human action), economic, social and technological developments and policy-driven actions, both at the domestic and the international level*"(Renn & Klinke, 2004). Kaufman and Scott defined Systemic risk as to the risk of probability of breakdown in the entire system and is evidenced by correlation among most or all parts (Kaufman & Scott, 2003). The use of route redistribution in local area networks makes it possible to connect different routing protocols, leading to a correlation among the protocols. Fan et al. claim that interrelated systems will likely increase the systemic risk level within the systems through a complex network of relationships.

A firm that uses route redistribution to connect different routing protocols within a local area network, going in line with Fan et al. claims, due to a systemic effect of interconnected systems, the likelihood of routing failure will be amplified. Hellström 2003 studied the systemic aspects of technological innovation. He suggested that in an attempt to grasp the systemic character of many technologies, it is useful to separate various types of technological change to see how these relate to each other (Hellström, 2003). Since the society is now so much dependent on networked data, there is a need to lay more emphasis on systemic risk which is a risk that affects the systems on which the society depends on. One way to govern the systemic risk is by using the risk governance framework presented below. For Discussions on systemic risk, see ((Acemoglu, Ozdaglar, & Tahbaz-Salehi, 2015; Battiston, Gatti, Gallegati, Greenwald, & Stiglitz, 2012; Bisias, Flood, Lo, & Valavanis, 2012; X. Fan, Wang, & Wang, 2020; Lehar & Alfred, 2005)). But I will exclude Risk Communication and Stakeholder and Public involvement because it is not relevant for this Thesis.

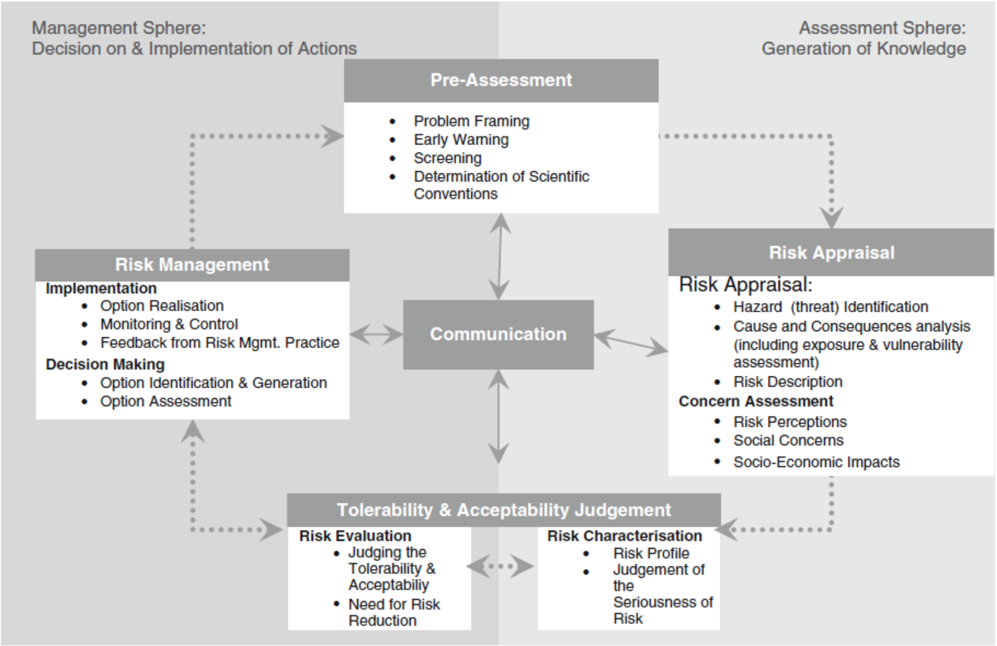


Figure 1: Risk Governance Framework (adopted from Renn,2008).

1.11 **Pre-Assessment:**

This deals with problem framing, where framing in the technical aspect of risk comprises the selection and interpretation of phenomena as relevant risk topics (Kahneman & Tversky, 1979). When there is an error or lack of background knowledge in the problem framing, the probability of an unpleasant event's occurrence will be high. Risk managers often search for the most efficient strategy to deal with risks; Public regulators often use pre-screening activities to allocate risks to a predefined procedure (Ortwin Renn & Aven, 2008). The method employed by public risk regulators can be beneficial to risk managers when searching for the most efficient strategy, for it can help place the perceived risk into different classes. For example, in chapter two (2), WBGU, as adopted from Renn et al. 2004, placed different risk perceptions into different classes using Greek mythology such as Sword of Damocles, Cyclops, Pythia, Pandora's box, Cassandra and Medusa.

1.12 **Risk Appraisal:**

Three main keywords come to mind when we talk about risk appraisal. These are Complexity, Ambiguity, and Uncertainty. Complexity is mostly used to address the highly related causal relationships, Uncertainty of cause-effects, and the plurality of interpretations, which ranges from the obvious (i.e., well-known cause-effects) to the unknowns (Ortwin Renn & Aven, 2008). The unknowns (surprises) here can be what is termed "BLACK SWANS," according to Taleb. For discussions on black swans, see (Aven, 2013b, 2014, 2015a). If we know all the cause-effect relationships, it will be easy to establish a scientific model that can address the complexity to some level of certainty. For example, if all the cause-effect relationships of various routing protocol failures are known in advance, scientific models that address each of the protocols can easily be established to some level of certainty. Certainty refers to some degree of confidence in predictions after all the necessary actions/methods have been carried out to understand and reduce complexity (Ortwin Renn & Aven, 2008).

Several discussions about Uncertainty in risk context have been carried out by several authors (see (Aven, 2013a; Bjerga et al., 2016)). Complexity and certainty/uncertainty are linked in a way, but ambiguity adds a different dimension to the characterization process. *"…Ambiguity refers to the degree of controversy associated with the interpretation of the assessment results and the evaluation of the tolerability or acceptability of the risk…"*(Ortwin Renn & Aven, 2008). The interpretation of the assessment results here can be greatly influenced by the way risk is perceived. According to Hellstrom 2009, risk perception affects how risk is realized, sustained, or reduced (Hellström, 2009). It is important to have a group of personnel with a common interest in interpreting the risk assessment results. Finally, risk appraisal starts with screening, which assumes the degree to which complexity, Uncertainty, and ambiguity are present (Ortwin Renn & Aven, 2008).

1.13 Risk Assessment

This involves identifying and exploring the types, intensities, likelihood, and consequences of an undesirable event such as routing failures. According to Renn et al., it is defined as *"…a tool of gaining knowledge about possible events and their consequences…"*(Ortwin Renn & Aven, 2008). A similar definition is made by Arthur Hayes, where he defined as the *"characterization of the potential adverse health effects of human exposures to environmental hazards"*(Hayes., 1993). He is clearly defining it with human health, but this can be used in this context as the characterization of possible failures of different routing protocols within a route redistribution.

1.14 **Risk Characterization and Evaluation**

Risk characterization and evaluation aim to make a judgment about risk acceptability and/or tolerability. It follows immediately after the risk appraisal stage in order to reach a balance, value-based judgment on the tolerability/acceptability of risk or to perform a trade-off analysis of a set of functional equivalents (of the product, process, or practice under consideration) and to initiate a management process and make preliminary suggestions for the most suitable management approach (Ortwin Renn & Aven, 2008). Risk is mostly evaluated with the traffic light model developed by the Health, Safety, and Environment (HSE), shown in Figure 3.2 below. Renn et al., 2004 claim that it is not in general advisable to stick with the normal traffic light model (Renn & Klinke, 2004) i.e., three categories for handling risks: the normal area, the intermediate area, and the intolerable area. Considering the task of generating, legitimizing and communicating risk management strategies, risks with one or several extreme qualities need special attention, so such similar risk phenomena are subsumed under one risk class in which they reach or exceed the same extreme qualities. They adopted the six classifications of risk clusters proposed by the German Scientific Advisory Council for Global Environmental Change (WBGU 2000), which is illustrated with Greek Mythology, which includes Risk Class Sword of Damocles, Cyclops, Pythia, Pandora's box, Cassandra and Medusa. The six classes demonstrate the complex issues associated with the new self-awareness of creating the future rather than just being exposed to fate. For example, The two risk classes Damocles and Cyclops require mainly science-based management strategies. The risk class Cyclops is a combination of risk-based and precautionary strategies, Pythia and Pandora demand precautionary principle, and the risk classes Cassandra and Medusa requires discursive strategies for building consciousness, trust, and credibility.

1.15 Risk Characterization

Risk characterization determines the evidence-based component for making the necessary judgment on the risk tolerability and /or acceptability, which should be seen beyond computed probabilities and expected values (Ortwin Renn & Aven, 2008). Justifying a judgment about the tolerability or acceptability of a given risk is a controversial aspect of handling risk. As defined in Renn et al., 2008; "…*The term* ***tolerable*** *refers to an activity that is seen as worth pursuing (for the benefit it carries), yet it requires additional efforts for risk reduction within reasonable limits. The term* ***acceptable*** *refers to an activity where the remaining risks are so low that additional efforts for risk reduction are not seen as necessary…*"(Ortwin Renn & Walker, 2008). Due to this controversy, it is important to follow the guidelines, as stated in Renn and Aven, 2008, when characterizing risk. It includes (Ortwin Renn & Aven, 2008):

- Expressed risk using probabilities and expected values, together with the background knowledge (assumptions and models).
- Descriptions of uncertainties in underlying phenomena and processes
- Potential outcome scenarios including the social and economic implications
- Assurance of compatibility with legal prescriptions
- Risk-risk comparisons and risk-risk trade-offs (how is risk in one area affected by changes in another area)
- Identification of discrepancies between risk assessment and risk perceptions as well as of potential equity violations.

There are uncertainties within any probabilistic estimates. Raphael et al., 2020, developed a method to incorporate uncertainties as an aid to support decisions (Raphael et al., 2020). Abdo et al. studied the effects of Uncertainty and compare different approaches to uncertainty treatments, where they claim that uncertainty quantification approaches can lead to different representations of Uncertainty in the outputs and, therefore, to different decisions (Abdo, Flaus, & Masse, 2017). A similar study was carried out by Helton et al., 2006 where he said that the uncertainty analysis is the determination of Uncertainty associated with the result of an analysis which is derived from Uncertainty related to the input to the analysis including the methods and models used in the analysis (Helton, Johnson, Sallaberry, & Storlie, 2006). This argument is justified by (Shortridge, Aven, & Guikema, 2017), where they presented a probabilistic bound assessment of Uncertainty, which ranges from Aleatory, Epistemic, and the combination of both. The two levels of Uncertainty, Aleatory Uncertainty where the risk estimates of an event taking place in the future are known on a group level but difficult to predict whether there will be a link failure in network routing or not. Secondly, Epistemic Uncertainty is the Uncertainty around the risk estimates where little is known on the risk estimates (Abdo et al., 2017; Aven, 2015a). Epistemic uncertainties can be reduced with further studies of the system, and the study on how to deal with epistemic Uncertainty is presented by (Galante, La Fata, Lupo, & Passannanti, 2020; Morales-Torres, Escuder-Bueno, Serrano-Lombillo, & Castillo Rodríguez, 2019). Bjerga et al., 2016 studied the uncertainty treatment in risk analysis of a complex system using System-theoretic accident model and processes (STAMP) and Functional Resonance Analysis Method (FRAM). The key finding is that the approach reduces the potential for surprises by increasing the system and risk understanding but need to be supplemented with other approaches by taking into account a more qualitative approach to address Uncertainty by making judgments on the strength of the background knowledge (see (Aven, 2014; Aven & Reniers, 2013; Bjerga et al., 2016)) to adequately support the decision-making on risk issues (Bjerga et al., 2016).

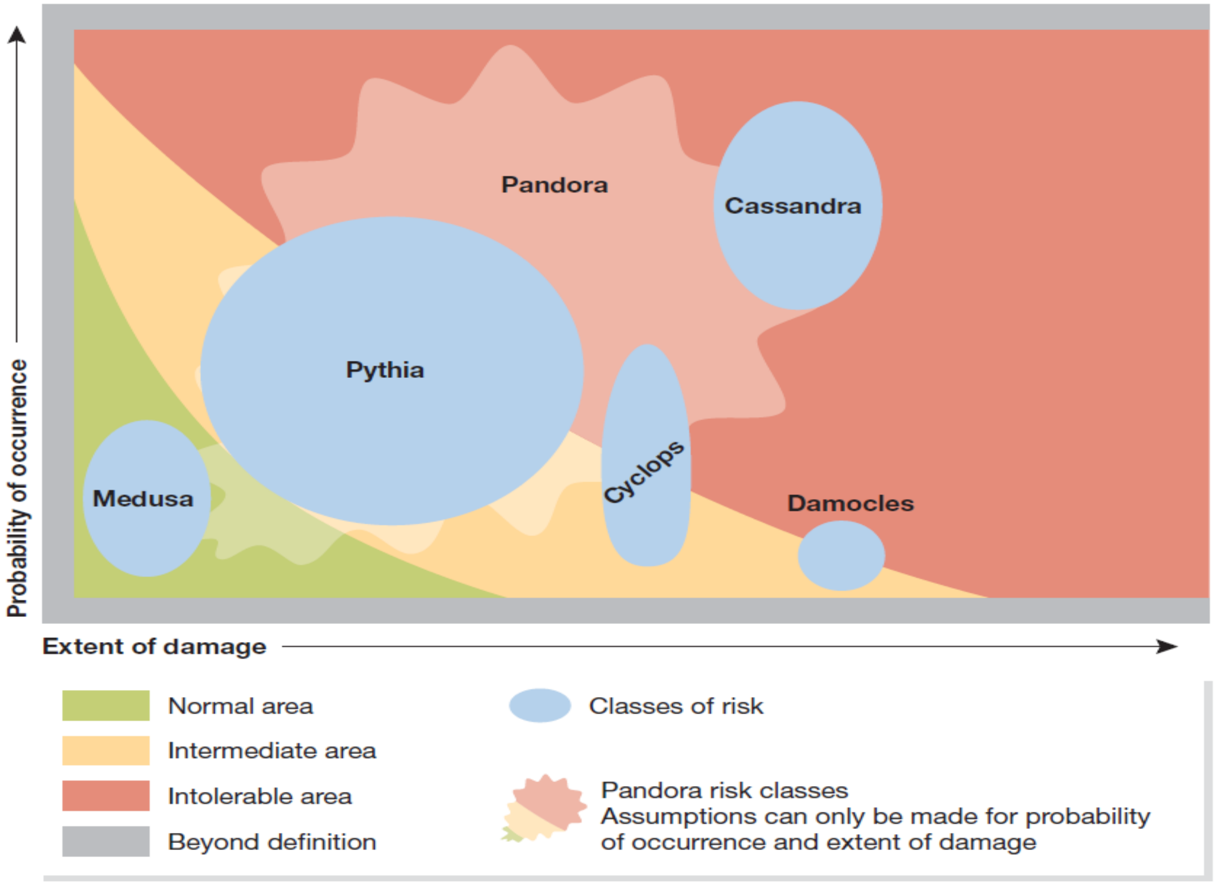


Figure 2: Risk classes

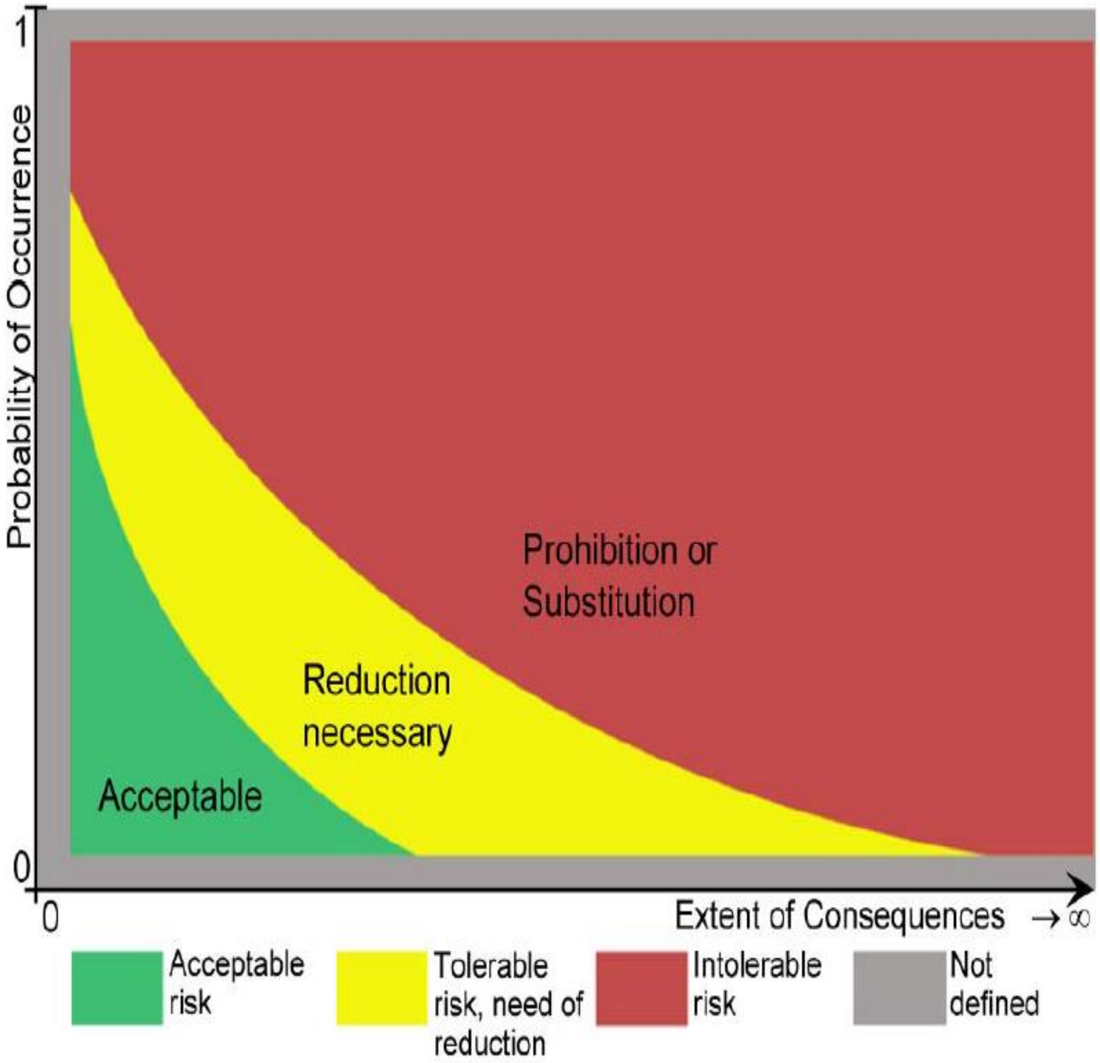
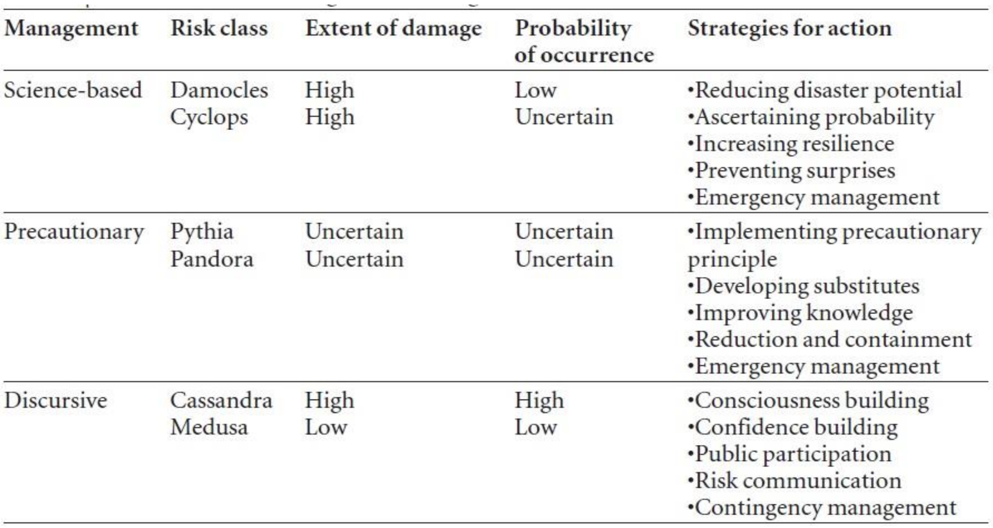


Figure 3: The traffic light model. Source (Ortwin Renn & Walker, 2008)



Management	Risk class	Extent of damage	Probability of occurrence	Strategies for action
Science-based	Damocles Cyclops	High High	Low Uncertain	•Reducing disaster potential •Ascertaining probability •Increasing resilience •Preventing surprises •Emergency management
Precautionary	Pythia Pandora	Uncertain Uncertain	Uncertain Uncertain	•Implementing precautionary principle •Developing substitutes •Improving knowledge •Reduction and containment •Emergency management
Discursive	Cassandra Medusa	High Low	High Low	•Consciousness building •Confidence building •Public participation •Risk communication •Contingency management

Figure 4: Management Strategies. Source (Ortwin Renn & Walker, 2008)

1.16 Risk Evaluation

While Risk characterization determines the evidence-based component for making the necessary judgment on the tolerability and/or acceptability of risk, Risk evaluation determines the value-based component for making this judgment. The evaluation helps to broaden the picture so as to include pre-risk aspects such as the social need for the specific risk agent, potential for conflict resolution, choice of technology, political priorities, etc. (Ortwin Renn & Walker, 2008). The evaluation aims to arrive at a judgment on tolerability and acceptability, which is based on balancing the advantages and disadvantages, discussing different development options for networks and routing, weighing the competing arguments and evidence claims in a balanced manner. "…*It should be noted that this elaborate procedure is only necessary if tolerability and/or acceptability is disputed and if society faces major dissents and conflicts among important stakeholders. If so, the direct involvement of stakeholders and the public will be a prerequisite for successful risk governance…*"(Ortwin Renn & Walker, 2008).

1.17 Risk Management

Risk management deals with the task of reducing, preventing, and altering the consequences identified by the risk assessment by choosing appropriate actions (Ortwin Renn & Aven, 2008). A similar definition was given by Terje Aven 2015, where he defined it as "*the process and implementation of measures to modify risk, including tools to avoid, reduce, optimize, transfer and retain risk*"(Aven, 2015b, p. 6). Here, he uses risk transfer as buying of insurance, i.e., transferring the risk to a better positioned party to carry it, but risk transfer is not relevant to this Thesis. According to Van Gestel and Baesens, 2008, it is a broad term to control the risk to the extent possible (Van Gestel & Baesens, 2008).

For a company that uses route redistribution, risk management should play a key role in selecting the routing protocols within the route redistribution. The results of the risk assessments of the various protocols will serve as a basis for the management. One should be careful when performing risk management for if it is not applied appropriately and consistently, risk management makes good risk managers appear as pessimists and naysayers, whereas those who take no proactive posture on risk are regarded as team players (Pritchard & PMP, 2014).

CHAPTER 2

2.1 Networking Concepts

In our day to day life activities, we communicate with different people, share our ideas, make new friends, etc. this is Networking. The term networking can be defined as the interconnection of people, computer gadgets, and an organisation for communication. In computing, Networking is the sharing of voice, video, data and printers, remote multimedia presentations and conferencing, etc.

Networking's sole purpose is to make connections between a PC and a printer or between a laptop and the internet. The true value of networking in the computing world comes from the traffic flowing over those connections. Consider a sampling of applications that can travel over a network's connections File sharing between two computers (Sequeira., 2018).

- Video chatting between computers located in different parts of the world.
- Surfing the web (for example, to use social media sites, watch the streaming video listen to an internet radio station, or do research for a school term paper).
- Instant messaging (IM) between computers with IM software installed.
- Voice over IP (VoIP), to replace traditional telephony system
- Control commands from the base computer to network equipment
- Email.

Unless everyone who needs to share network, resources are in the same office space (uncommon situation), the challenge is to connect relevant networks so all users can share the wealth of whatever services and resources are required. For Networking to be achieved, several components should be in place, and these are listed as follows. Client, Server, Hub, Switch, **Routers**, Media, WAN links. For the definition of the listed network components, see (Lammle, 2016; Sequeira., 2018), and I will limit my attention to **routers** only for this Thesis.

A network can be divided into segments or more general networking term *subnets*. A subnet is a logical subdivision of an IP network into two or more networks.

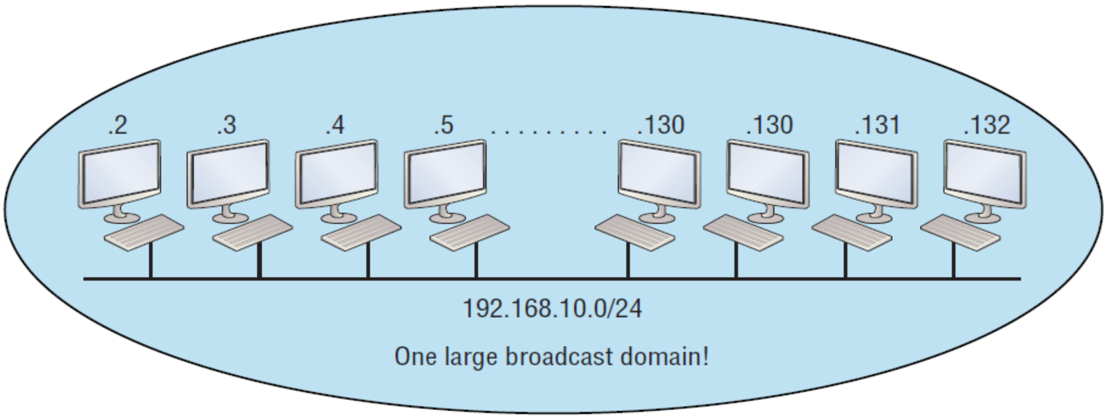


Figure 5. A single network (subnet), One large broadcast domain. Source (Lammle, 2016)

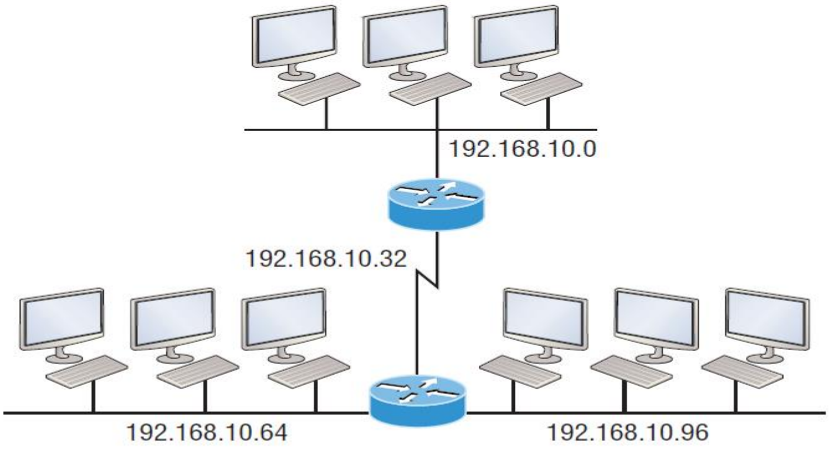


Figure 6. Three subnetworks, three broadcast domains. Source (Lammle, 2016).

Figure 1.1 is a large network with 132 computers that belongs to a single broadcast domain. A broadcast domain is a logical sub-division of computer networks in which all nodes can reach each other through broadcast. Figure 1.2 is three (3) networks with three (3) computers each. Therefore, a subnet divides a network into different broadcast domains.

2.2 Router

A router is the networking device that forwards data packets between computers in different broadcast domains. Using figure 2 as an example, computers in 192.168.10.64 network can communicate with each other but cannot communicate to those on 192.168.10.96 and 192.168.10.0 networks without the use of routers. Routers in figure 2 provide the link between the three (3) subnetworks. Let us see how this works in the real world.

Consider the Faculty of Science and Technology at the University of Stavanger as one (1) large network; this large network is divided into subnetworks e.g., Department of Risk Management, Department of Industrial Economics, and Department of Petroleum Engineering. Using figure 2 above, assuming the Department of Risk Management belongs to 192.168.10.64 network, the Department of Industrial Economics and the Department of Petroleum Engineering belongs to 192.168.10.96 and 192.168.10.0 networks, respectively. A computer in the Risk Management network can communicate with another computer in risk management without routing (e.g., Fredrick's Computer can easily communicate with Stine's Computer without routing). However, for communication between different departments to go through, it must pass through a routing process.

2.21 Routing Process:

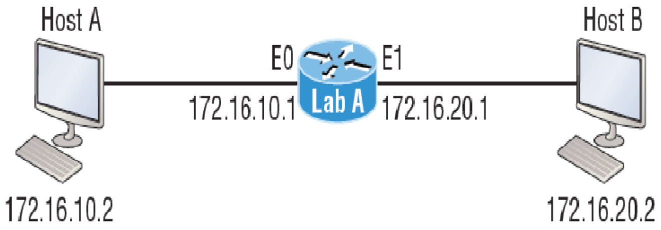


Figure 7 routing process. Source (Lammle, 2016).

From fig. 3 above, Host A in 172.16.10.0 network with an IP address of 172.16.10.2 and a default gateway of 172.16.10.1 (i.e. interface E0 of router Lab A) wants to communicate with host B in 172.16.20.0 network with an IP address of 172.16.20.2 and a default gateway of 172.16.20.1(interface E1 of Lab A router).

The internet protocol (IP) creates a packet. Once the packet is created, IP determines whether the destination IP address is on the same network or a different network. Since the IP address is on a different network, the packet must be sent to the default gateway (E0 interface of the Lab A router), so it can be routed to a different network (172.16.20.0). But for this packet to be sent to the default gateway, the hardware address of the router's interface E0 with an IP address of 172.16.10.1, must be known. Why? The packets can be handed down to the datalink layer, framed, and sent to the router's interface connected to the 172.16.10.0 network.

The reason for this is that hosts communicate only through hardware addresses on the local network, it’s important to recognize that for host A to communicate to host B, it has to send packets to the Media Access Control (MAC) address of the default gateway on the local network.

IP Address	172.16.10.2
MAC Address	0030.9492.a4ac

Table 1: IP to MAC Address mapping

Address resolution protocol (ARP) is used to map IP Address to MAC Address just as in table 1.1 above. Next, the Address Resolution Protocol (ARP) cache of the Host is checked to see if the default gateway has already been resolved to a hardware address. If the IP to MAC address mapping has not been resolved, Host sends an ARP request to the router interface connected to host A (interface E0), and the router responds with an ARP reply message containing the MAC address of E0 interface. Once the IP address of the default gateway is mapped to the MAC address, the packet will be handed into the data link layer for framing then sent to the router E0 interface.

IP Address	MAC Address	Interface	Type
172.16.20.1	00d0.58ad.05f4	E1	ARP_A
172.16.20.2	0030.9492.a5dd	E1	ARP_A
172.16.10.1	00d0.58ad.06aa	E0	ARP_A
172.16.10.2	0030.9492.a4ac	E0	ARP_A

Table 2. Arp table of Lab a router.

When the frame gets to the router through the E0 interface, the router consults its routing table to see if the destination IP is in the same subnet with Host A. From table 2. above, the destination IP 172.16.20.1 is on a different subnet (see (Lammle, 2016; Sequeira., 2018) for discussion on subnetting), and it is connected to interface E1 (Ethernet 1) of the router which is the exit route configured by the system administrator. The router then checks its ARP table to know if the IP of

Host B has been resolved to a MAC address, as shown in table 2. The packet will now be sent to the data link layer for framing and forwarding.
The simple routing process explained above is only feasible in a small network with only one router, and this is no longer possible in today's network, even the simplest home network contains two or more router as shown in fig 1.5 and 1.6 below, e.g., consider a complex network with about 1000 workstations with 32 subnets and 30 routers.

The system administrator will have to configure an exit route for 32 subnets on 30 routers, and whenever there is a topological change in the network, which is inevitable in today's network, he/she will have to reconfigure 30 routers (Static Routing). It does not scale well in the large and growing network, and this leads us to different routing process called Dynamic Routing.

2.22 Dynamic Routing

Dynamic routing uses protocols to find networks and update routing tables on routers. Manually adding rout information in a large network does not scale well. Fortunately, a variety of dynamic routing protocols allow a router's routing table to be updated as the network conditions change. What does this mean? Let us look at the fig 8 below.

Let us assume that the workstation 10.10.10.0/24 with the CORP router is in the university library, and the SF router with 10.10.20.0/24, which is on a different subnet, is in the department of Risk Management. For communication to go between someone in the library and someone in the Risk Management Department, the two routers must communicate their route information. E.g., SF router will tell the CORP router, hey, if you can to get to network 10.10.20.0/24, use me, and the CORP will tell the SF router, hey, if you want to get to 10.10.10.0/24 network, use me. Therefore, when someone from the University library sends a message to someone in the department of risk management because the CORP knows the way (route) to get to the library, it will just send the packet through its s0/0 interface. When there is a change in the network condition, e.g., change in subnet from 10.10.20.0/24 to 10.10.30.0/24, the periodic communication between routers enables them to have an updated route each subnet.

A routing protocol defines the set of rules used by a router when it communicates routing information between neighboring routers (Lammle, 2016). Just as in fig. 8, the SF router uses routing protocols to communicate routing information with the CORP router. These routing protocols belong to some sort of classes. Let us look at the different classes of routing protocols below.

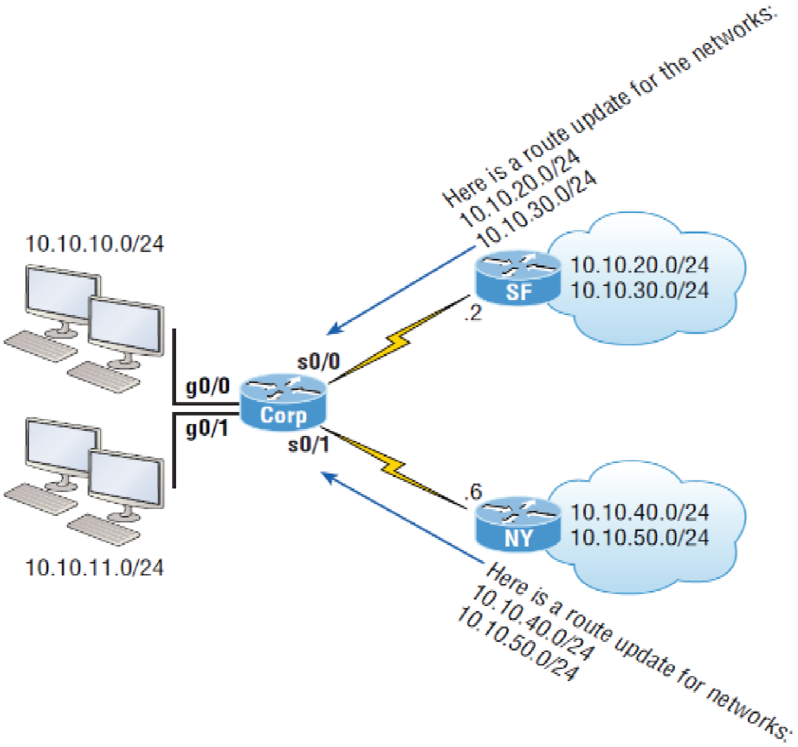


Figure 8, routing process 2. Source (Lammle 2016)

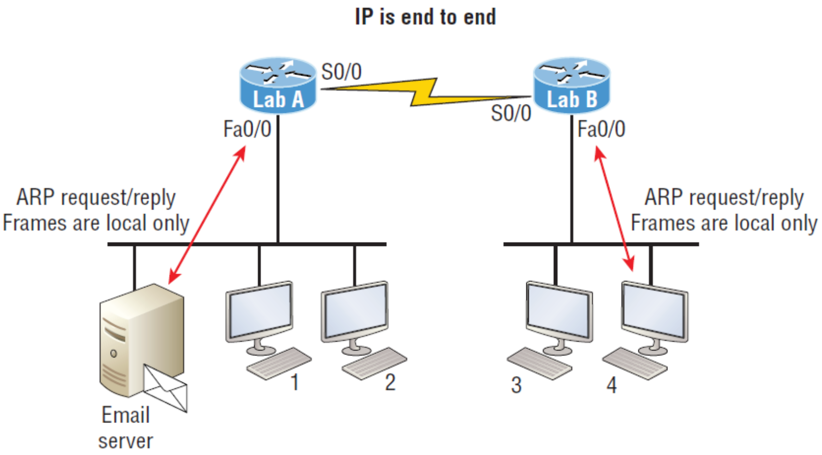


Figure 9. Routing process 3. Source (Lammle 2016)

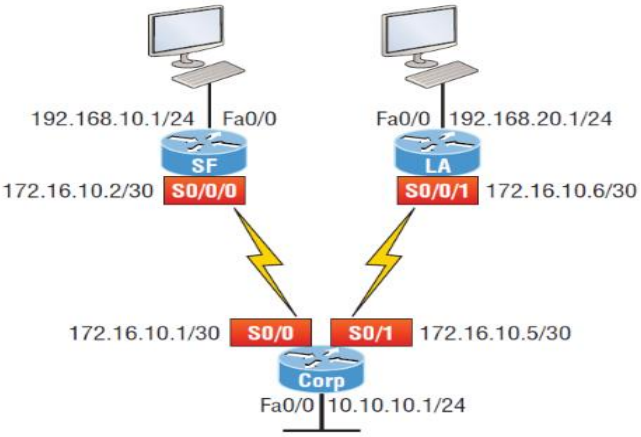


Figure 10. Routing process 4. Source (Lammle, 2016)

2.3 Classes of Routing Protocols:

There are three classes of routing protocols: Distance vector, Link State and Advanced Distance Vector. These are based on some type of metric called an Administrative Distance (AD), which is used to rate the trustworthiness of routing information received on a router from a neighboring router. If both advertised routes to the same network have the same AD, then routing protocol metrics like hop count and/or bandwidth of the lines will be used to find the best path to the remote network. What does this mean?

Consider two road networks that lead to University of Stavanger (point C) from Stavanger City Centre as A and B, number of bump stations as the hop count (which is also the number of routers on the way to the destination) and the traffic of each route as the bandwidth. If it takes 20km (AD) from point A to point C and 27km (AD) from B to C., point A will be taken as the optimal route, but if it takes 20km from A to C and 20km from B to C, seven bump stations from A to C and five bump stations from B to C. Point B will be considered as the optimal route. Or if the traffic from B to C is higher than the traffic from A to C, then A to C will be considered the optimal route. Now let us look at the various classes of routing protocols.

2.31 Distance Vector

Distance vector protocols use *Bellman-Ford algorithms* to finds the best path to a remote network by judging distances. The vector indicates the direction of the remote network. Each instance where a packet goes through a router is called a hop, and the path with the least number of hop counts to the remote network will be chosen as the best route. It uses *hello* messages to discover directly connected neighbors.

This protocol sends a full copy of its routing table to its directly connected neighbor routers. This is a periodic advertisement, which means that even if there is no topological change to the network, a distance-vector protocol will, at regular intervals, advertise its full routing table to its neighbors again. The two major problems with this protocol are routing loop and counting to infinity. The Bellman-Ford computation induces the looping in a distributed environment, and it occurs when a link fails (Medhi & Ramasamy, 2007). The type of risk here is classified as a known known type of risk, according to Taleb.

2.32 Link State

Link state protocols, also known as Shortest Path First (SPF) protocol is based on Dijkstra's algorithm to compute the shortest path to a destination. The protocol uses three tables to determine the optimal route to a destination. One table keeps track of the directly attached neighbors, one determines the topology of the entire internetwork, and one is used as the routing table. There is no periodic exchange of routing tables, such as in distant vector protocols. Instead, triggered updates as a result of topological changes containing only specific link state information are sent. Periodic keepalives that are small and efficient, in the form of hello messages are exchanged between directly connected neighbors to establish and maintain neighbor relationships (Lammle, 2016). This approach only uses a selected set of paths, and this is a trade-off between storage and complexity. By storing multiple candidate paths ahead of time, the actual computation is simple when new link costs are received. Such a candidate path-based approach can potentially miss a good path. There are special cases where a routing loop can also occur. In the risk context, this is seen as the known unknowns (i.e., events known by some experts but unknown to some). One cannot neglect the negative implications of this known unknown type of risk, for it may cause an unexpected consequence.

2.33 Advanced Distance Vector

Advanced distance vector protocol is a kind of combination of a distance vector protocol and link-state protocol in that it uses the traditional *hello* message to form a neighbor relationship just as in distance vector protocol and again only partial updates are sent whenever a topological change occurs which is a characteristic of the link-state protocol.

2.4 Types of Routing Protocol

There are two types of routing protocols: Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP). The Interior protocols operate under an autonomous system, where an autonomous system is a network under single administrative control.

2.41 Routing Information Protocol, Version 1 (Ripv1)

This is the first routing protocol used in a TCP/IP-based network in an intradomain environment. RIP belongs to the distance-vector routing protocol class, and it relies on hop count (number of intermediate routers) to determine the best way to a remote network, but with a maximum allowable hop count of 15 by default meaning that you cannot have more than 15 routers within the intra-network for RIP to function properly. RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask, which results from RIPv1 not sending route updates with subnet mask information to its neighbors. This makes RIP super inefficient on large networks with slow WAN links or networks with many routers installed and completely useless on networks that have links with variable bandwidth.

RIP remains the most popular routing protocol in a small office home office environment where the links are ***unlikely*** to fail; this means looping is unlikely to occur. But how to quantify the likelihood of a link failure here is a question yet to be answered. There could be surprises. If a link or an interface card is likely to fail, RIPv1 faces serious transient issues, including possibly creating black hole routers (Medhi & Ramasamy, 2007).

2.42 Routing Information Protocol, Version 2 (Ripv2)

This routing protocol is an improvement to RIPv1 because it uses classless routing, which means that it supports variable length (classless) subnet masking, unlike RIPv1 that uses classful subnet mask. This is achieved with something called Prefix routing and does send subnet mask information with its route updates (classless routing), but it still faces looping problem just as in RIPv1 and with 15 hop count limits.

2.43 Open Shortest Path First (OSPF)

OSPF is an instance of a link-state protocol based on hop-by-hop communication of routing information, specifically designed for intradomain routing in an IP network (Medhi & Ramasamy, 2007). Such a routing protocol requires information about the state (e.g., cost) of a link, and the ability to advertise this link-state reliably through in-band communication. OSPF is an open standard routing protocol that has been implemented by a wide variety of network vendors, including Cisco. The open standard characteristic is the key to OSPF's flexibility and popularity. OSPF allows for the creation of areas and autonomous systems, minimizes routing update traffics, is highly flexible, versatile, and scalable, It offers unlimited hop counts unlike RIP versions 1 and 2. The most useful trait of OSPF is that its design is intended to be hierarchical in use, meaning that it allows us to subdivide the larger internetwork into smaller internetworks called areas, as shown in fig 1.7 below.

The idea behind the OSPF hierarchical design is to keep route updates to a minimum, especially in a larger network, and this also keeps problems from propagating throughout the network, effectively isolating them from a single area. Since it belongs to the family of a link-state routing protocol, it also experiences the same problems associated with link-state routing protocols. OSPF routers will only become neighbors if their interfaces share a configured network to belong to the same area number. The risks here are the issue of misconfiguration, especially when you must deal with a large number of routers.

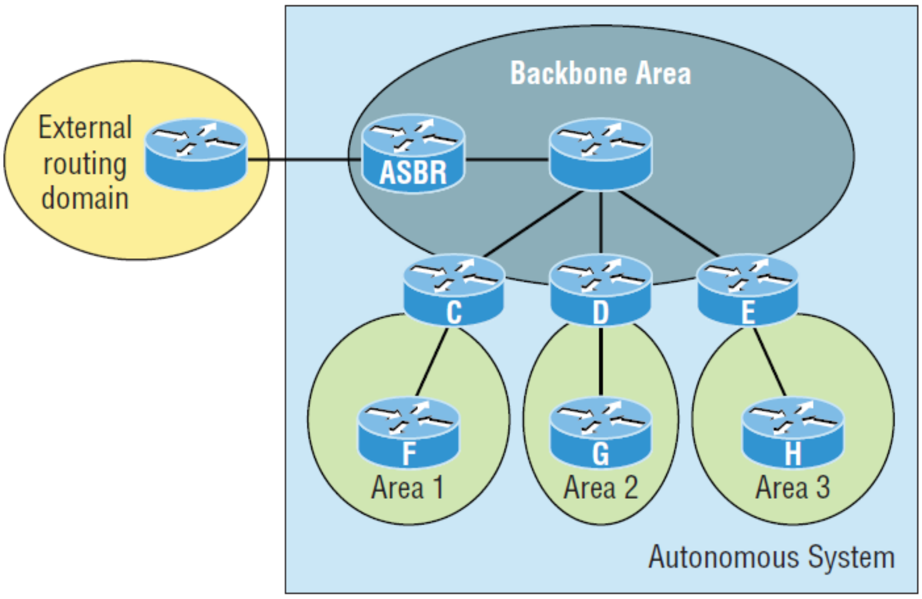


Figure 11. OSPF Routing. Source (Lammle, 2016)

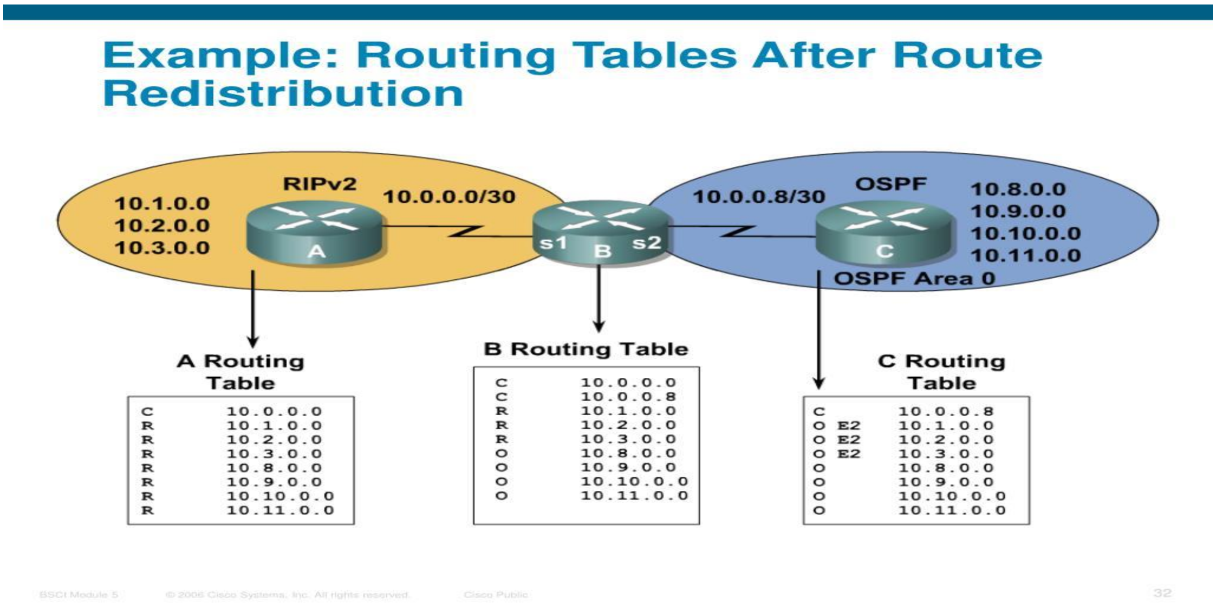
2.44 Enhanced Interior Gateway Protocol (EIGRP)

This is a routing protocol developed by Cisco, but it is not an open standard routing protocol. This routing protocol belongs to the distance vector protocol family, but it provides a loop-free routing, which is accomplished using a diffusing computation algorithm. There is an active coordination phase before routing computation when a link fails or links cost changes; to do that, additional information is sought for which the diffusing update algorithm (DUAL) needs to maintain states that allow EIGRP to attain faster convergence (Medhi &

Ramasamy, 2007). This protocol requires a reliable delivery to function best, so to achieve that, a reliable multicast mechanism is used.

2.5 Route Redistribution

Route redistribution is used in our network today to connect two networks that speak different routing protocols. E.g., the routes (IP prefixes) of the network running OSPF routing protocol can be learned by another network using EIGRP and vice versa. The benefit is that when one network learns about another network's IP prefix, it can forward any user traffic to addresses in the other network. To learn about routes, a router at the boundary that is connected to both networks is required to perform route redistribution which means that the router redistributes routes it has learned from the first network to the second network using the routing protocol used by the second network (Medhi & Ramasamy, 2007).



A Routing Table

```
C       10.0.0.0
R       10.1.0.0
R       10.2.0.0
R       10.3.0.0
R       10.8.0.0
R       10.9.0.0
R       10.10.0.0
R       10.11.0.0
```

B Routing Table

```
C       10.0.0.0
C       10.0.0.8
R       10.1.0.0
R       10.2.0.0
R       10.3.0.0
O       10.8.0.0
O       10.9.0.0
O       10.10.0.0
O       10.11.0.0
```

C Routing Table

```
C       10.0.0.8
O E2    10.1.0.0
O E2    10.2.0.0
O E2    10.3.0.0
O       10.8.0.0
O       10.9.0.0
O       10.10.0.0
O       10.11.0.0
```

Figure 2 Route Redistribution between RIPv2 and OSPF. (Image adapted from slideplayer.com)

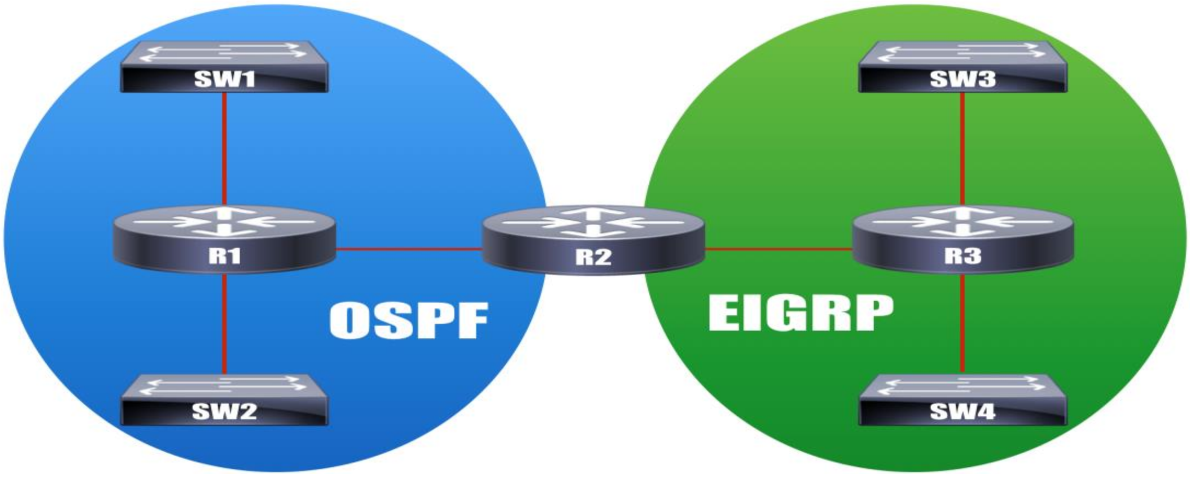


Figure 3 Route Redistribution between OSPF and EIGRP. (image adapted from kwtrain.com)

The risk issues here might be a systemic effect, which is a risk of breakdown of the whole system propagating from one protocol to another. From a Helbing point of view, when networks are interdependent, they are more vulnerable to abrupt failures i.e., hyper-connected networks establish hyper-risks (Helbing, 2013). There might be cases where the EIGRP protocol's failure causes the failure of OSPF, or the failure of RIPv2 causes the failure of OSPF.

CHAPTER 3

3.1 Methodology

This chapter aims to give a general overview of the understanding of how the information gathering process has transformed. The information in this Thesis comes from peer-reviewed journals, books, and interviews from the professionals in the networking field.

Qualitative research was performed in this Thesis, and the qualitative research method used is a teleconferencing interview with the working professionals in the networking field. A total of nine (9) correspondents were interviewed and based on the research questions below, four (4) network administrators, three (3) network Engineers, and two (2) cisco certified networking associates were interviewed. The class of the professionals chosen is based on the research questions because they are better positioned to provide useful information regarding the research questions. For example, the network Engineers are responsible for the design of the network; they make decisions on how the network will be with given criteria and how the network should be managed. The system administrators oversee the periodic functioning of the network, and the cisco networking professionals mostly work in the data centers where they mostly handle and maintain the hardware such as routers.

RESPONDENTS	BACKGROUND
Respondent 1	Network Administrator: Circle K MSc Computer Science: University of Warsaw Poland. CompTIA network+: CompTIA CCENT: Cisco
Respondent 2	Network Administrator: Circle K Poland. MSc InfoTech: University of Warsaw Poland. CompTIA network+: CompTIA
Respondent 3	Network Administrator: Globacom Nigeria. BSc Computer Science: University of Ibadan Nigeria. CompTIA A+, network+: CompTIA CCENT: Cisco CCNA: Cisco
Respondent 4	Network Administrator: Globacom Nigeria. BSc Computer Engineering: Covenant University Nigeria. CompTIA network+: CompTIA
Respondent 5	Network Engineer: Beyond.pl Poland

	BSc Computer Science: University of Warsaw Poland. MSc Big Data Science: Kozminski University. Warsaw, Poland. Assert Management: Udemy.com
Respondent 6	Network Engineer: 3s (3s.pl) data centre Poland. BSc Data Science and Business analytics: University of Warsaw Poland. CCENT, CCNA, CCIE: Cisco
Respondent 7	Network Engineer: Airtel Nigeria. BSc Computer Engineering: Covenant University Nigeria. Network Management: Airtel Nigeria CCENT, CCNA, CCIE: Cisco CompTIA Network+: CompTIA
Respondent 8	System Administrator: MTN Nigeria BSc Electrical and Electronic Engineering: Anambra state university Nigeria. CCNA: Cisco
Respondent 9	System Administrator: MTN Nigeria. BSc Electrical and Telecom Engineering: Nnamdi Azikiwe University Awka Nigeria.

Table 3: Background information of the respondents.

Search Engine:	Search – Keywords:
oria.no	Risk Analysis
	Risk Governance
	Black swans
Sciencedirect.com	Risk Governance
	Systemic Risk
	Risk and Globalisation
	Risk and Technology
	Risks associated with globalisation
	Risks and Networks
	Deep Uncertainty
Google scholar	Systemic risk of globalisation
	Vulnerability and risk
	System theoretic accident model and processes
	Functional resonance analysis method.
	Risk governance and complex systems
	Systemic risk
	Effects of globalisation
Wiley.com	Deep Uncertainty
z-lib.org	Networking concepts
	Risk assessment
	Routing fundamentals
	CCNA routing and switching
	CompTIA network+

Table 4. Search engines with search keywords

3.2 **Limitations of The Study:**

The method chosen for this study is to provide a broad overview of the current risk governance practice with regards to Networking. Several emails were sent out to different companies in Norway for a face to face interview or for teleconferencing. However, because of the partial lockdown in Norway that resulted in companies working from home, it was difficult to schedule an interview session with most of the networking companies in Norway because I was not getting any replies to the emails I sent out. Secondly, I had wanted to have a record of the interview sessions with some of the network engineers in the field, which could have helped in a better analysis of the results, but the request was turned down by the correspondents for personal reasons.

CHAPTER 4

4.1 Results:

There are several reasons behind the use of different routing protocols within cooperation or a firm.

Five (5) respondents said that they use OSPF and RIPv2 within their network because of their branch offices' geographical dispersion. Since the branch offices consist of many routers which are geographically spread out, thus, manageability and scalability is an important issue. Therefore, it is desirable to have the ability to cluster the entire domain into several subdomains by introducing hierarchy. OSPF provides this functionality to divide an intradomain network into subnetworks, commonly referred to as *areas*. OSPF does not work so well with older routers due to high memory and CPU requirements. Therefore, routing protocol such as RIPv2 is used in some places where there are old routers.

Three (3) respondents said that they use EIGRP, OSPF, and RIPv2 within their network due to new acquisition (i.e., acquiring an existing company) that already runs a different routing protocol. Instead of going through the rigorous process of change, they opted for a quick and temporal solution to integrate the various protocols using route redistribution.

One (1) respondent said that they use EIGRP and OSPF within their networks because they have routers from different vendors (Cisco, Huawei) and because EIGRP is Cisco proprietary routing protocol until recently it was made an open standard, it does not work well in a router from a different vendor. With the reasons given above, one can say that the use of a single routing protocol within a network is nearly impossible and this makes the protocols to be interconnected/interdependent with each other through route redistribution. In line with Dirk Helbing 2013, when networks are interdependent, they are more vulnerable to abrupt failures i.e., hyper-connected networks establish hyper-risks (Helbing, 2013). If this risk interdependence can be properly analyzed, then substantially effective risk response decisions can be made (Kwan & Leung, 2011).

Some respondents said that when a link fails, routing protocols such as RIPv1 and RIPv2 experience a routing loop i.e., a situation where a data packet continues to go in a circular motion within routers without getting to its destination. When this happens in a LAN that uses route redistribution, it creates a ripple effect within the system where the problem propagates from one protocol to another through route redistribution. If the problem is not resolved quickly, it can cause a total breakdown of the system. Some correspondents said that in some situation where a router reboots itself due to overheating or some other unexplainable cause if it is a cisco router running OSPF or RIPv2, it requires the intervention of the network administrator to reconfigure the routing metrics because, by default, Cisco routers use EIGRP metrics for routing. In a situation where the network administrator is not available when the problem occurs, this causes routing loops within the network because routers will not know where to send their routing information due to bad metrics, and this problem will also propagate from one routing protocol to another creating a systemic effect. Fan et al. claim that due to a systemic effect of interconnected systems, the likelihood of routing failure will be amplified.

Different routing protocol uses a different metric to calculate the best route to a network, so there is always a convergence problem and looping. The network administrators configure the boundary routers to translate the metric value from one protocol to another by assigning static administrative distance to the protocols. The main findings here is that there is no standard risk governance framework for the management of network routing within the industry. They use what is available to them without considering the negative consequence that may occur in the long run.

CHAPTER 5

5.1 Analysis of Result:

It is almost impossible to use only a single routing protocol in our local area networks today. The use of different routing protocols in LAN resulted in the use of the complex system Route Redistribution. Route redistribution aids the communication between different protocols but, at the same time, adds to the complexity of the network. Benefits offered by route redistribution comes at the cost of contagion risk, which is a core part of systemic risk. "*Governance of systemic risks requires strategies that address the complexity, scientific uncertainty, and socio-political ambiguity of its underlying relationships*" (Renn, 2016). This has created a Systemic Risk within LAN networks i.e., the risk of a breakdown in the whole system as a result of the correlation among all parts of the system (Kaufman & Scott, 2003) or the risk of experiencing strong systemic event where such an event adversely affects several systemically important intermediaries (Renn & Klinke, 2004). From this point of view, the failure of a protocol says RIPv2 in a route redistribution can cause the failure of OSPF and that of EIGRP and vice versa, showing that an event adversely affects the number of systemically important intermediaries. The main findings here are that the benefits of route redistribution come at the cost of the contagion effect, which is a core part of systemic risk.

There is a need for systemic risk consideration during the design and management of networks beyond the normal traffic light model to the six classes of the risk presented in Renn and Klinke, 2004, where they said that "…*The ultimate aim of classifying risks is to draft feasible and effective strategies for risk management and to provide measures for policies on different political levels…*" (Renn & Klinke, 2004). A complex system's problem is that potential failures in a complex system cannot be predicted accurately by just looking at the series of component failures that may occur (Nancy G Leveson, 2011).

We should investigate the system functions and try to establish the relationships amongst various components of the system. In line with Hellström 2003, in an attempt to grasp the systemic character of many technologies, it is useful to separate various types of technological change to see how these relate to each other (Hellström, 2003). I chose the literature (Bjerga et al., 2016), where the STAMP and FRAM give attention to dependencies that cover a range of system aspects. STAMP and FRAM methods are used to develop a model of the system and the system behavior, including potential system failures, which can be presented to a decision-maker. But this is just a model representing potential failures; therefore, there are some uncertainties concerning this potential failure e.g., how likely are the scenarios? Good decision making is based on proper understanding and treatment of uncertainties, but how do we convey the message about uncertainties?

Probabilities are the most popular tool to represent uncertainties, but the use of probabilities in the risk analysis of a complex system is a strong debate among experts (Aven, Baraldi, Flage, & Zio, 2013; Hollnagel, 2012; Nancy G; Leveson, Daouk, Dulac, & Marais, 2003) but abandoning probabilities can lead to ignoring important aspects of risk and Uncertainty, therefore, a poor decision-making (Bjerga et al., 2016). I chose the use of knowledge-based probabilities (subjective probabilities) supplemented with the assessment of the strength of knowledge suggested by Terje Aven because it is impossible to monitor the network under similar conditions, which is a requirement for objective (frequentist) probabilities. The risk classes developed by the German Scientific Advisory Council for Global Environmental Change (WBGU 2000) will be used in characterizing the risk, for it will help to draft a good strategy for management. The next chapter starts with a presentation of the STAMP and FRAM model, A real-world case scenario, and the STAMP and FRAM model's application to the case.

5.2 Functional Resonance Analysis Method (FRAM):

This is a method to develop a system model and its behavior, including potential system failures or accidents. The key elements of FRAM used for risk analysis are (Hollnagel, 2012):

1. Identify and describe essential system functions.
2. Assess variability for each function
3. Assess how the variability of multiple functions can be coupled and lead to nonlinear outcomes (what is referred to as functional resonance).
4. Identify countermeasures.

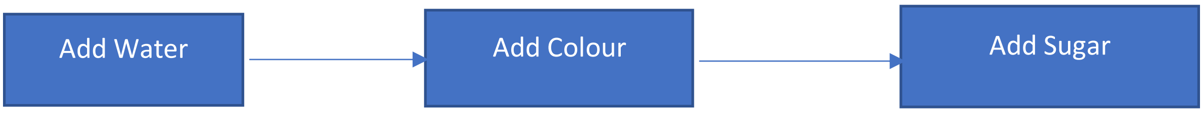
5.3 System Theoretic Accident Model and Processes (STAMP):

The analysis has the following structure (Nancy G Leveson, 2011):

1. Identify the accidents to be considered, the system-level hazards, safety constraints, and functional requirements.
2. Create a model of the functional control structure for the system in question
3. Identify the potential unsafe control actions (unsafe control of the system)
4. Determine how each potentially hazardous control action from step 3 could occur, i.e., the scenarios leading to unsafe control.

5.4 Case 1:

Consider a juice production company that uses a time-sensitive (i.e., a certain event must happen at a certain period) robotic equipment for her daily operation. There are three events in their production network i.e., Add Water, Add Colour, Add Sugar.



These events happen at a specific time interval as the juice bottle train (as shown in fig. 4 below) passes through each module. The production network and the marketing network are interconnected to get a clear overview of customers' requests and stocks. The production network is using the EIGRP routing protocol; the marketing network uses the RIPv2 routing protocol. Route Redistribution is used to connect the two networks here.

Unfortunately, there is a routing failure in the marketing department due to a traffic surge. This failure propagates to the production network through route redistribution and causes a failure in the EIGRP routing protocol. Due to the fast convergence of EIGRP, it fails and comes back up quickly, but the *transient* time between failure and re-convergence causes three modules to malfunction. Because the module is time-sensitive, there are a series of undesirable events which is calculated with the combination formula shown below.

nℂr (n combination r) = $\frac{n!}{r!(n-r)!}$

where n = number of modules = 3,

r = n-*i*; where *i* ranges from 0 to n-1 (0,1…,n-1).

This gives $3\mathbb{C}3 + 3\mathbb{C}2 + 3\mathbb{C}1 == \frac{3!}{3!(3-3)!} + \frac{3!}{2!(3-2)!} + \frac{3!}{1!(3-1)!} == 1 + 3 + 3 = 7$

The table below shows a combination of 7 undesirable events.

Water	Colour	Sugar
Yes	Yes	No
Yes	No	Yes
No	Yes	Yes
Yes	No	No
No	Yes	No
No	No	Yes
No	No	No

Table 4: Combination of Undesirable events.

This means a situation where some juice will have water and color without Sugar, water, and Sugar without color, color, and Sugar without water and so on.

Figure 4: A train of juice. Image adapted from fruitprocessingline.com

5.5 Discussion

One of the main features of systemic risks is the ripple effect beyond the domain in which the risks originally appear and the threat of multiple breakdowns of important or critical services to society (Renn, 2016). This can be seen from case 1 above, where the failure of the RIPv2 routing protocol of the marketing department causes the failure of the EIGRP routing protocol in production.

Returning to the case 1, step 1 of FRAM provides a qualitative and textual model of the system and how it operates in a daily (failure-free) system constructed around the concept of functions (Bjerga et al., 2016). From the case presented above, the control of the production module is one function provided by the control computer; the transfer of information is another function provided by the EIGRP protocol. Dependencies between various functions are referred to as 'couplings' in the FRAM world (Bjerga et al., 2016). Step 2 and 3 are central, including the sources and outcomes of this variability, and how multiple functions' variability can be coupled and cause failure. Functional variability is a smooth adjustment that aims to deal with everyday challenges in a complex world (Hollnagel, 2012). These adjustments can be for the good of the system, but there are uncertainties about the outcome of such adjustments, which can be the very source of why things go wrong (Bjerga et al., 2016). The variability, in this case, can be for many reasons. E.g., EIGRP protocol can fail and remain in a failure state for a long time; the route redistribution system can fail due to high load, the production module can malfunction due to overheating. All these variations can occur simultaneously, thereby producing excessive variability and failures.

This method produces a model of the system and specific potential accident scenarios that can be presented along with countermeasures to the decision-makers. Applying the STAMP to the case above, the high traffic on RIPv2 protocol represents a system hazard to the route redistribution. Therefore, the safety constraint is to monitor the traffic closely and switching it off from route redistribution when it fails. The failure can occur if the system administrator does not uphold the safety constraints. Step 2 is to create a model of the system's functional control structure to illustrate how it can still fail if the safety constraints are not upheld. Step 3 is to identify potential inadequate control actions that could lead to failed states, e.g., the system administrator can assign a wrong administrative distance to the route redistribution. Step 4 is to identify further how potentially hazardous control actions can occur and identify the causes. The result of the analysis is a list of scenarios of bad control actions, conditions for when they become unsafe and causes of these hazards, which can be used to suggest and evaluate mitigating measures, which is then handed over to the decision-makers (Bjerga et al., 2016).

The risk governance framework presented in chapter one (1) is one of the major frameworks suitable in governing complex systems and systemic risk, but there is a need to go beyond the normal traffic light model in classifying risk. The six risk classes developed by the WBGU and as presented in Renn et al. 2004 aim to classify risks to develop practicable and effective strategies for risk management (Renn & Klinke, 2004).

Let us assume we have seven (7) modules in production network, the rate of the undesirable events will be:

$7\mathbb{C}r = \frac{7!}{r!(7-r)!} == 1 + 7 + 21 + 35 + 35 + 21 + 7 = 127.$

The case considered is that it fails and comes back up quickly; what if the problem persists for a long period, the outcome will be a chaotic uncertainty. "*Chaotic uncertainty is too high a price to pay for somewhat higher average levels of prosperity*" (Nye. & Donahue, 2000).

There is need to see beyond the classic technological risk aspect which is based on probabilities and extent of damage to an adaptive risk governance process that lays more emphasis on systemic risk which requires a more holistic approach to hazard identification, to risk assessment and to risk management because systemic risks are complex, stochastic and nonlinear (Renn, 2016). Let us apply the risk governance framework presented in chapter one (1) to the example presented in the previous chapter and see how things unfold.

Pre-Assessment:

This deals with problem framing, where framing in the technical aspect of risk comprises the selection and interpretation of phenomena as relevant risk topics (Kahneman & Tversky, 1979). From case 1 above, the use of route redistribution within the industry created systemic risk within the LAN. One must be careful during the routing protocol selection process, especially when these protocols are to be connected to a sensitive network within the industry and not to be dependent on fate, as is the case of most industries. Systemic risk was not taken into consideration during the design process of the network. Attention should be given to the systemic events present in route redistribution during the risk governance process. For example, using a protocol such as OSPF in the marketing.

Risk Appraisal:

The three main keywords in risk appraisal are complexity, ambiguity, and Uncertainty. This Thesis focuses on Uncertainty only. Uncertainty of the cause-effects and plurality of interpretations ranges from the obvious to the unknowns (Ortwin Renn & Aven, 2008). The routing protocols presented in chapter two have different characteristics and so different uncertainties. E.g., RIPv2 protocols are more prone to routing loop than EIGRP, EIGRP still fails due to an Unknown cause, and in some rare situation, it still experiences routing loop. OSPF uses areas to limits the propagation of routing problems. The use of route redistribution to connect these protocols makes the network more complex, and such complex systems are affected by pervasive Uncertainty, which may lead to a surprising effect (Bjerga et al., 2016). Uncertainty treatment in risk analysis of complex systems (STAMP and FRAM) presented in the previous chapter can be used to model Uncertainty here, but the problem is that the model largely excludes the use of probabilities. In risk analysis, it is normal to resort to probabilities while conveying the message about uncertainties.

Risk Characterisation:

This determines the evidence-based components for making the necessary judgment on the risk tolerability and /or acceptability, which should be seen beyond computed probabilities and expected values (Ortwin Renn & Aven, 2008). It is difficult to justify the tolerability or acceptability of systemic risk using the normal traffic light model. It is important to see beyond the traffic light model and rather focus on the six classes of risk when trying to characterize systemic risk.

Applying risk classes to the case 1 presented, it is difficult to say how tolerable the risk is for a combination of RIPv2 and EIGRP or OSPF and EIGRP or RIPV2, OSPF and EIGRP protocols due to the systemic effect on the whole network through route redistribution. But with risk classification, one can say that the case presented belongs to the risk class Pythia and Pandora or Cyclops because the extent of damage caused by the systemic event to the system is great or uncertain and the probability of occurrence is uncertain.

The risk classification above is there to develop a feasible and effective strategy for risk management and to provide measures for policies on different political levels (Renn & Klinke, 2004). The risk here requires a science-based and precautionary approach. This Thesis focuses only on two of the methods, which are: Ascertaining probabilities, preventing surprises.

Management Strategies:

- Ascertaining probabilities
- Preventing Surprises.

Ascertaining Probabilities:

probability is one of the controversial topics in risk management. When one talks about probabilities, it is important to distinguish which of the probabilities he/she is referring to i.e., subjective, objective, or imprecise probabilities (see (Aven, 2015a; Aven et al., 2013; Aven & Reniers, 2013)).

In objective(frequentist) probability, it deals with a situation where something is repeated several under similar conditions (such as the Urn model referred to in Aven, 2015). The problem here is the term "*similar conditions*" because there is no way to get the routing protocol working under similar conditions. The activities of humans determine the traffic that flows through it.

The subjective (knowledge-based) probability is the degree of belief that an event will occur. It is not fruitful to say that the probability of failure of the EIGRP protocol is 0.01 without knowing how the various components of the system work. The systemic nature of route redistribution greatly affects the behavior of each protocol. Therefore, the FRAM and STAMP model presented above helps increase the system knowledge, and this will help to have a broad understanding of the system's functional components. But there is a need to assess the strength of knowledge here. The strength of the knowledge assessment suggested in Aven,2015, is shown below.

Knowledge is Strong when:

- The degree to which assumptions made represent strong simplifications.
- The availability of relevant data
- The degree of agreement/consensus among experts
- The degree of understanding of the phenomena involved
- The existence of accurate models (Aven, 2015a).

The problem with complex systems is that they cannot be understood only based on the probability model's components; the interconnections or relationships among parts are always missing (Bjerga et al., 2016). The STAMP and FRAM model addresses many of this issue.

<u>Preventing Surprises:</u>

Aven T described black swan as "*a surprisingly extreme event relative to one's belief/knowledge*." There are three main types of the black swan:

a) Events that were unknown to the scientific environment (Unknown unknowns)
b) Events not on the list of known events from the perspective of those who carried out a risk analysis (or another stakeholder), but know to others (unknown knowns i.e., unknown events to some, known to others)
c) Events on the list of known events in the risk analysis but judged to have a negligible probability of occurrence, and thus not believed to occur (Aven, 2013b, 2019; Aven & Krohn, 2014).

To solve the problem of possible surprises or black swan, we need to balance risk-based approaches, cautionary/precautionary, and discourse-based approaches only in cases where the knowledge is very strong and the uncertainties small, can the risk-based approach be used alone (Aven, 2014).

CHAPTER 6

6.1 Conclusion:

It is important for risk personnel to consider system risk during the complex system's risk governance process. The use of route redistribution in our networks today causes a series of systemic events on the network. We saw from the case presented how the RIPv2 protocol's failure causes the failure of EIGRP protocol in the production network and the series of undesirable events that occurred. From the data gotten during the interview session, it is inevitable to avoid the use of route redistribution in today's network, and this is where a better risk governance strategy comes into play. Governing systemic risk requires a more holistic approach to hazard identification, risk assessment, and management. Risk analysis for systemic risks must focus on interdependencies, ripple, and spillover effects (Horlick-Jones & Sime, 2004).

Pre-assessment helps in making a better choice of routing protocols within route redistribution. This frames the problem as systemic. Knowing fully well that RIP protocols are susceptible to failure in a high traffic network, with systemic effect in mind, the use of RIPv2 in the marketing department would have been avoided. OSPF which is less susceptible to failure due to high network traffic.

Risk appraisal conveys the message about uncertainties within the system. The FRAM and STAMP model helps to model the system functions, which will provide a broad understanding of the whole system and its various dependencies for easy risk identification. For example, the uncertainties within OSPF protocol, the type of network it controls, the type of router it operates on, the type of protocol it is connected to through route redistribution, and the type of network the other protocol controls. The message about Uncertainty should be conveyed to the decision-maker.

The risk characterization should go beyond the normal traffic light model due to the systemic effect of the identified risk and focus on the six classification of risk. These six classifications help draft feasible and effective strategies for risk governance/management and provide policies on different political levels. One of the policies here may be the use of EIGRP protocols only on a CISCO router since it does not work so well on a router from a different vendor, thereby creating uncertainties on the reliability of the protocol.

The results of the characterization process influence the management strategies here. It is difficult to use probabilities to access uncertainties within the system due to the stochastic nature of systemic risk. But the assessment of uncertainties, which is based on probabilities, is supplemented with improving knowledge with the FRAM and STAMP model and assessing the strength of the underlying knowledge developed by Aven T and considering the potential surprises.

The use of the risk governance framework will improve the management of route redistribution by following the framework judiciously from pre-assessment to risk management. The knowledge about the uncertainties between different protocols will help to limit the frequency of routing failures in our network by not using protocols such as RIPv2 in a high traffic network, not using EIGRP in a non-cisco router, making a better choice of protocols that will be in route redistribution.

6.2 Recommendation:

From risk governance and management perspective, it will be fruitful to have routing protocols that use a single metric as a standard for route calculation, for this will reduce the potential for possible systemic effect due to negligence on the part of system administrators. This can also serve as a basis for further research—for example, *the effects of globalized routing metrics from a risk perspective*.

It is also important for companies to have a policy on the type of routers they use within their network. For example, if they must use EIGRP protocol, they should consider using only cisco routers within the network since EIGRP does not work so well on a router from another vendor, but other protocols work well on a cisco router.

Reference

Abdo, H., Flaus, J. M., & Masse, F. (2017). Uncertainty quantification in risk assessment - Representation, propagation and treatment approaches: Application to atmospheric dispersion modeling. *Journal of Loss Prevention in the Process Industries, 49*, 551-571. doi:https://doi.org/10.1016/j.jlp.2017.05.015

Ač, A. (2010). The End of Growth: Systemic Risks of Globalization. *The New Presence*(3), 49-52.

Acemoglu, Ozdaglar, & Tahbaz-Salehi. (2015). Systemic risk and stability in financial networks. *American Economic Review, 105*(2), 564-608.

Angst, C. M., Agarwal, R., Sambamurthy, V., & Kelley, K. (2010). Social contagion and information technology diffusion: The adoption of electronic medical records in US hospitals. *Management Science, 56*(8), 1219-1241.

Archibugi, D., & Pietrobelli, C. (2003). The globalisation of technology and its implications for developing countries: Windows of opportunity or further burden? *Technological Forecasting and Social Change, 70*(9), 861-883. doi:https://doi.org/10.1016/S0040-1625(02)00409-2

Aven, T. (2013a). On How to Deal with Deep Uncertainties in a Risk Assessment and Management Context. *Risk Analysis, 33*(12), 2082-2091. doi:10.1111/risa.12067

Aven, T. (2013b). On the meaning of a black swan in a risk context. *Safety Science, 57*, 44-51. doi:https://doi.org/10.1016/j.ssci.2013.01.016

Aven, T. (2014). *Risk, Surprises and Black Swans: Fundamental ideas and concepts in risk assessment and risk management.* London and New York: Routledge.

Aven, T. (2015a). Implications of black swans to the foundations and practice of risk assessment and management. *Reliability Engineering & System Safety, 134*, 83-91. doi:https://doi.org/10.1016/j.ress.2014.10.004

Aven, T. (2015b). *Risk Analysis*: John Wiley & Sons, Ltd.

Aven, T. (2019). The cautionary principle in risk management: Foundation and practical use. *Reliability Engineering & System Safety, 191*, 106585. doi:https://doi.org/10.1016/j.ress.2019.106585

Aven, T., Baraldi, P., Flage, R., & Zio, E. (2013). *Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods*: John Wiley & Sons.

Aven, T., & Krohn, B. S. (2014). A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering & System Safety, 121*, 1-10.

Aven, T., & Reniers, G. (2013). How to define and interpret a probability in a risk and safety setting. *Safety Science, 51*(1), 223-231. doi:https://doi.org/10.1016/j.ssci.2012.06.005

Battiston, S., Gatti, D. D., Gallegati, M., Greenwald, B., & Stiglitz, J. E. (2012). Liaisons dangereuses: Increasing connectivity, risk sharing, and systemic risk. *Journal of economic dynamics and control, 36*(8), 1121-1141.

Bisias, D., Flood, M., Lo, A. W., & Valavanis, S. (2012). A survey of systemic risk analytics. *Annu. Rev. Financ. Econ., 4*(1), 255-296.

Bjerga, T., Aven, T., & Zio, E. (2016). Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliability Engineering & System Safety, 156*, 203-209. doi:https://doi.org/10.1016/j.ress.2016.08.004

Fan, M., Lin, N.-P., & Sheu, C. (2008). Choosing a project risk-handling strategy: An analytical model. *International Journal of Production Economics, 112*(2), 700-713. doi:https://doi.org/10.1016/j.ijpe.2007.06.006

Fan, X., Wang, Y., & Wang, D. (2020). Network connectedness and China's systemic financial risk contagion——An analysis based on big data. *Pacific-Basin Finance Journal*, 101322. doi:https://doi.org/10.1016/j.pacfin.2020.101322

Galante, G. M., La Fata, C. M., Lupo, T., & Passannanti, G. (2020). Handling the epistemic uncertainty in the selective maintenance problem. *Computers & Industrial Engineering, 141*, 106293. doi:https://doi.org/10.1016/j.cie.2020.106293

Hayes., A. H. (1993). *Risk Assessment in Federal Government: Managing the Process*. In (pp. 206).

Helbing, D. (2013). Globally networked risks and how to respond. *Nature, 497*(7447), 51-59.

Hellström, T. (2003). Systemic innovation and risk: technology assessment and the challenge of responsible innovation. *Technology in Society, 25*(3), 369-384. doi:https://doi.org/10.1016/S0160-791X(03)00041-1

Hellström, T. (2009). New vistas for technology and risk assessment? The OECD Programme on Emerging Systemic Risks and beyond. *Technology in Society, 31*(3), 325-331. doi:https://doi.org/10.1016/j.techsoc.2009.06.002

Helton, J. C., Johnson, J. D., Sallaberry, C. J., & Storlie, C. B. (2006). Survey of sampling-based methods for uncertainty and sensitivity analysis. *Reliability Engineering & System Safety, 91*(10), 1175-1209. doi:https://doi.org/10.1016/j.ress.2005.11.017

Hollnagel, E. (2012). *FRAM, the functional resonance analysis method: modelling complex socio-technical systems*: Ashgate Publishing, Ltd.

Horlick-Jones, T., & Sime, J. (2004). Living on the border: knowledge, risk and transdisciplinarity. *Futures, 36*(4), 441-456.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. *Econometrica, 47*(2), 263. doi:10.2307/1914185

Kaufman, G. G., & Scott, K. E. (2003). What is systemic risk, and do bank regulators retard or contribute to it? *The Independent Review, 7*(3), 371-391.

Kwan, T. W., & Leung, H. K. (2011). A risk management methodology for project risk dependencies. *IEEE Transactions on Software Engineering, 37*(5), 635-648.

Lammle, T. (2016). *CCNA Routing and Switching*. Canada: Wiley & Sons, Inc., Indianapolis, Indiana.

Lehar, & Alfred. (2005). Measuring systemic risk: A risk management approach. *Journal of Banking & Finance, 29*(10), 2577-2603.

Leveson, N. G. (2011). Engineering a safer world: systems thinking applied to safety (engineering systems). *MIT Press Cambridge*.

Leveson, N. G., Daouk, M., Dulac, N., & Marais, K. (2003). Applying STAMP in accident analysis.

Mann, A., Kauffman, R. J., Han, K., & Nault, B. R. (2011). Are there contagion effects in information technology and business process outsourcing? *Decision Support Systems, 51*(4), 864-874.

Medhi, D., & Ramasamy, K. (2007). *Network Routing: Algorithms, Protocols, and architectures.* In (pp. 957).

Morales-Torres, A., Escuder-Bueno, I., Serrano-Lombillo, A., & Castillo Rodríguez, J. T. (2019). Dealing with epistemic uncertainty in risk-informed decision making for dam safety management. *Reliability Engineering & System Safety, 191*, 106562. doi:https://doi.org/10.1016/j.ress.2019.106562

Neumann, P. G. (1994). *Computer-related risks*: Addison-Wesley Professional.

Nye., J. S. j., & Donahue, J. D. (2000). *Governance in a Globalizing World*. In (pp. 401).

Ortwin Renn, & Aven, T. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. London. Sterling, VA: earthscan.

Ortwin Renn, & Walker, K. D. (2008). *Global Risk Governance. Concept and Practice Using the IRGC Framework*. Dordrecht, Netherlands: Springer.

Peters, K., Buzna, L., & Helbing, D. (2008). Modelling of cascading effects and efficient response to disaster spreading in complex networks. *International Journal of Critical Infrastructures, 4*(1-2), 46-62.

Pritchard, C. L., & PMP, P.-R. (2014). *Risk management: concepts and guidance*: CRC Press.

Raphael, D. B., Russell, N. S., Immink, J. M., Westhoff, P. G., Stenfert Kroese, M. C., Stam, M. R., . . . Boersma, L. J. (2020). Risk communication in a patient decision aid for radiotherapy in breast cancer: How to deal with uncertainty? *The Breast, 51*, 105-113. doi:https://doi.org/10.1016/j.breast.2020.04.001

Renn, O. (2016). Systemic risks: The new kid on the block. *Environment: Science and Policy for Sustainable Development, 58*(2), 26-36.

Renn, O., & Klinke, A. (2004). Systemic risks: A new challenge for risk management. *EMBO reports, 5 Spec No*, S41-46. doi:10.1038/sj.embor.7400227

Renn, O., Lucas, K., Haas, A., & Jaeger, C. (2019). Things are different today: the challenge of global systemic risks. *Journal of Risk Research, 22*(4), 401-415. doi:10.1080/13669877.2017.1409252

Roberts, D. F. (1999). *Kids and media at the new millennium*: Diane Publishing.

Sequeira., A. (2018). *CompTIA Network+ N10-007 Cert Guide*.

Shortridge, J., Aven, T., & Guikema, S. (2017). Risk assessment under deep uncertainty: A methodological comparison. *Reliability Engineering & System Safety, 159*, 12-23. doi:https://doi.org/10.1016/j.ress.2016.10.017

Slovic, P. (2013). *Risk, media and stigma: Understanding public challenges to modern science and technology*: Routledge.

Sprinkel, S. C. (2001). Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime. *Suffolk Transnat'l L. Rev., 25*, 491.

Szymanski, B. K., Lin, X., Asztalos, A., & Sreenivasan, S. (2015). Failure dynamics of the global risk network. *Scientific reports, 5*, 10998.

Van Gestel, T., & Baesens, B. (2008). *Credit Risk Management: Basic concepts: Financial risk components, Rating analysis, models, economic and regulatory capital*: OUP Oxford.