Availability Incidents in the Telecommunication Domain: A Literature Review

Faiza Allah Bukhsh Eelco Vriezekolk Hans Wienen Roel Wieringa

Contents

Abstract

Non-availability incidents in public telecom services may have a wide-spread impact, such as disruption of internet services, mobile services, and land-line communication. This, in turn, may disrupt the life of consumers and citizens, and the provision of services by commercial and public organizations. These incidents are always analyzed and solved by the provider. In Europe, there is a legal obligation to report the analysis and solution of the incident to the national telecom regulator. However, these reports are highly confidential, and beyond some elementary descriptive statistics, they are not analyzed. This means that a significant opportunity is missed to draw lessons from these incidents, which could be valuable to other providers and to standardization bodies. In the LINC project [1], we aim to develop a method to draw lessons learned from registered non-availability incidents without compromising the confidentiality of those registrations. As a preparation for that, we have conducted a systematic literature review of non-availability incidents in public telecom services reported in the scientific and professional literature, to see what we can learn from the reported incident model and analysis methods used. In this report, we present an incident analysis taxonomy to establish a common terminological ground among researchers and practitioners.

1 Introduction

The availability of telecommunication infrastructure and the internet are essential concerns of society today. Partial or complete failure of these infrastructures may bring disruption of communication services. This, in turn, may lead to decreased quality of life for citizens and consumers. Moreover, it may lead to preventable loss of life and/or property damage by causing delays in emergency response and disaster relief efforts. Society's dependence on telecommunication services makes these services indispensable.

The critical availability of telecommunication infrastructure can be compromised by system malfunctioning, natural disasters, human mistakes, and attacks.

In Europe, Framework Directive 2009/140 of the European Union Agency for Network and Information Security (ENISA) requires European telecom providers to report major non-availability incidents to their national regulators (European Union Agency For Network And Information Security, 2017). These, in turn, report registered incidents yearly to the ENISA. For example, in the Netherlands, public telecom providers are obliged to report significant incidents and their resolution to the *Agentschap Telecom* (AT), which reports them to ENISA.

These incident reports are potentially beneficial to all telecom providers and to regulators, because they may involve common vulnerabilities in telecom infrastructures or standards that need to be repaired. However, the reports are highly confidential, and other than some descriptive statistics, no useful information is currently extracted from these reports.

The goal of the LINC (Learning from Incidents)[2] project is to develop a method to draw lessons learned from registered incident reports, without compromising the confidentiality of those reports. To prepare for this, we have conducted a systematic literature review to collect a list of published incidents, especially in the telecom domain. Our goal in this report is to extract from the literature a taxonomy of availability incident analysis methods and to summarize the root causes that have been reported.

The rest of this report is organized as follows, in section 2 we state the research questions and search strategy of our literature review. In section 3 we discuss the results of our literature review. In section 4 we summarize the answers to our research questions, discuss the validity, and sketch our future work.

2 Research Method

To perform the systematic literature review, we followed Kitchenham methodology (Kitchenham et al., 2015). To avoid confusion, we will start with defining the concept of an incident, then represent the research questions and finally explain our search string and search strategy.

[1] http://scs.ewi.utwente.nl/research/r_cybersecurity/LINC/
[2] http://scs.ewi.utwente.nl/research/r_cybersecurity/LINC/

2.1 The concept of an incident

The ISO 20000-1:2011 standard defines an incident as

> "an unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customers" (ISO, 2005).

We make two observations about this definition. First, the definition assumes that any unplanned interruption is undesired too. In this report, we make this assumption explicit and speak of unplanned and undesired interruptions.

Second, in most domains, an unplanned and undesired interruption to a service is called a *accident,* whereas an *incident* is usually defined as an unplanned and undesired event that did not result, or only minimally resulted, in a loss, damage or injury, due to favorable circumstances (Wienen et al., 2017). In this terminology, had the circumstances been different, it could have developed into an accident.

The concept of an incident is defined from service delivery to customers. A related concept is that of a *error,*, which is a deviation from a correct state (Avizienis et al., 2004). All incidents are errors, but some errors may not be classified as incidents, because no interruption of service took place. Errors, in turn, are caused by *faults,*, which are vulnerabilities in a system that need to be repaired.

However, in the telecommunications domain, the term "incident" includes what is elsewhere called an accident. Here, we focus on telecommunications, and therefore we will use the ISO definition, with the slight extension that incidents are undesired. So in this report, an incident is

> "an unplanned and undesired interruption to a service, a reduction in the quality of service, or an event that has not yet impacted the service to the customers."

2.2 Research questions

Our literature review aims to answer the following research questions:

- **RQ1:** What telecom incidents have been reported in the scientific literature?
- **RQ2:** What incident analysis methods have been used?
- **RQ3:** What root causes of telecom incidents have been reported?

2.3 Search strategy

We first selected Scopus as the digital library to use, because it contains publications from major journals and conference proceedings, which helped us get a diverse set of publications on the subject. A well-known bibliographic research (Harzing and Alakangas, 2016) and (Mongeon and Paul-Hus, 2016) indicated it as the most comprehensive and user-friendly database.

To develop a search string, we experimented with a variety of combinations of keywords to test synonyms used in literature (Kuhrmann et al., 2016). After several iterations we ended up with the following search string:

- Telecommunication AND Incident AND Analysis AND (Methods OR Method OR Approaches OR Approach OR Technique OR Techniques)

Using this search string, Scopus returned 291 results. We have applied the following restrictions to define the boundaries of our study: (i) limit by source type (i.e., conference papers and journal articles), and (ii) limit by subject area, i.e., Computer Science, Engineering or Business.

After we had settled on a search string, we extended our search to other four well-known digital libraries, namely IEEE Explorer, ACM, Springer, and ScienceDirect. This resulted in 488 publications in total (Figure 1). We then cleaned up this initial set in the following steps.

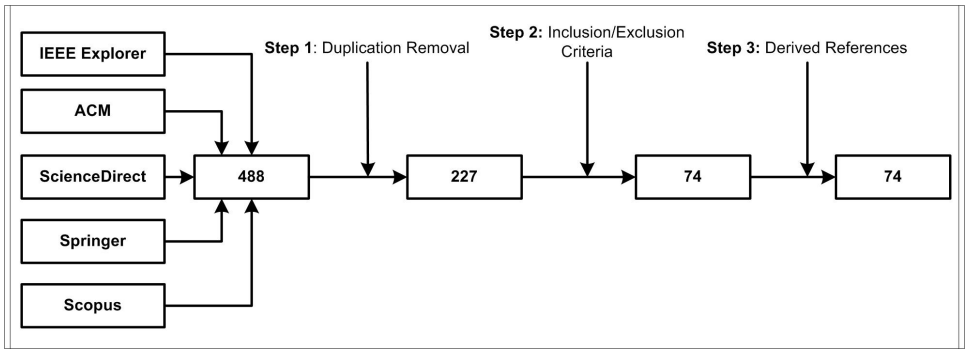

Figure 1: Literature Search Statistics

Step 1 Duplicate removal: After scrutinizing the 488 publications we found that 42% papers were duplicate. After discarding duplicates, we were left with 227 articles.

Step 2 Inclusion criteria: To find the most relevant papers, we have analyzed the titles and abstracts of 227 publication by using the inclusion criteria (IC) listed and motivated as follows. The application of the criteria reduced the set to 73 papers.

- **IC1**. The paper directly relates to the RQs of our review. **Motivation:**This means, we include papers that explicitly discuss an incident, and/or analysis method, approach, or technique. Additionally, we included only papers that highlight the root cause of an incident. Besides, if the root cause of an incident is being highlighted or not.
- **IC2**. A study in the form of a scientific peer-reviewed paper. **Motivation:** A scientific paper guarantees a level of quality through a peer-review process and contains a substantial amount of content.
- **IC3**. The objective of the study is presented/proposed method(s) for incident analysis. **Motivation:** We are interested in telecom incidents with a focus on how they are solved. A solution for this could be a complete list of best practices consisting of processes/methods/approaches/frameworks or solutions.
- **IC4**, The language of the literature, is either Dutch or English. **Motivation:** As this research is performed in the Netherlands.
- **IC5** Paper is available for download. **Motivation:** Most of the time, abstracts are available, but we cannot conclude all the details from an abstract only. Therefore we will consider only full papers.

Step 3 Trace references: To mitigate this risk of leaving out important information, we pursued the reference lists of all collected studies. We conclude that if we missed references by our restriction to five databases, then this literature is almost surely ignored by all research in these five databases.

We used the conceptual schema of Figure 2 to collect information from the papers and answer our research questions. The three relationships in the diagram are many to many, as indicated by the crow-foot.

3 Results

The complete list of the 74 papers, analyzed according to the schema of Figure 2 is given in Appendix A. This answers RQ1. In section 3.1 we summarize this answer briefly. The data needed to answer RQ2 and RQ3, extracted from these 74 papers, is listed in Appendix B. We summarize this in sections 3.2 (RQ2) and 3.3 (RQ3). Finally, appendices C and D list of examples of methods and techniques collected from the literature.

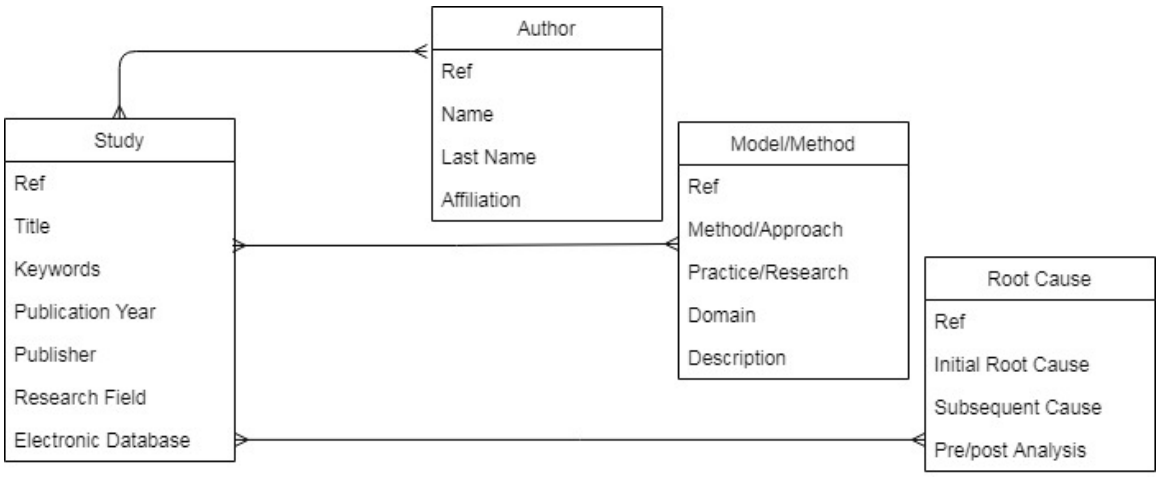

Figure 2: Literature synthesis conceptual model

3.1 RQ1 Published telecom incident analyses

We first classify the literature in several dimensions. Figure 3 shows the number of publications per year. Where before the year 2000 there was no more than one publication per year, in the decade after the year 2000 the number of publications increased to about 5 per year, with some random fluctuations per year. This clearly reflects the increased scientific interest in telecom availability incidents in that period, probably due to the advent of mobile communications and the rise of the Internet, both of which have increased the dependence of society on telecommunication services.

Next, we answer a number of exploratory questions about the literature.

- **Do the studies found only belong to the telecommunication Domain?** Forty studies discuss telecom incidents either directly or indirectly, but 34 studies examine how to use telecom services to prevent incidents in other domains (Figure 4). For example, Steenbruggen et al. discussed the use of data obtained from cellular phones to identify and mitigate traffic incidents in Amsterdam city (Steenbruggen et al., 2013).

- **Does the paper report about an industrial case study, about a method proposal, or a combination of both?** We classified the papers in four classes (Figure 5):

  1. Method proposal without motivation or validation in real-world cases (12 papers).
  2. Method proposal validated in a real-world case (0 papers- this is the gap in the market).
  3. Method proposal motivated by the analysis of real-world incidents (32 papers).
  4. Industrial case study without a method proposal (30 papers).

  This analysis shows there is a need for validation of method proposals in real-world case studies. For example, Fault tree analysis and task analysis have emerged from practice, and they are widely used. Research proposals typically focus on technical or on organizational aspects, but no method proposal integrates these aspects. 60% proposals focus on error detection, and 25% focus on error recovery. However, error recovery itself consists of error handling (removing the errors) and fault handling (preventing the fault from happening again) (Avizienis et al., 2004). None of the reviewed methods make this distinction.

- **What is the main focus of the study, risk analysis, or incident reporting?** Out of 74, 39 studies focused on risk assessment (pre-incident) rather than incident analysis (post-incident). Figure 6 shows the numbers.

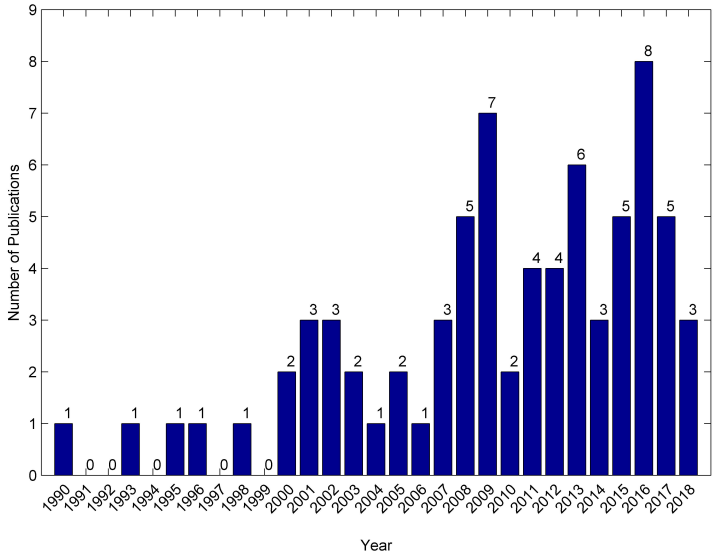

Figure 3: The number of publications per year.

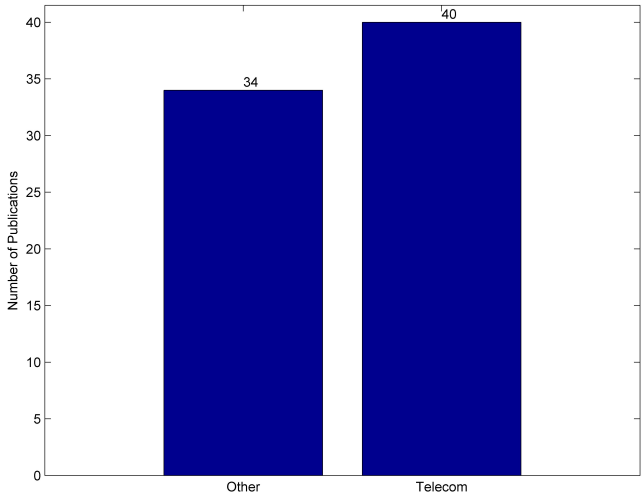

Figure 4: Domain specificity of the studies

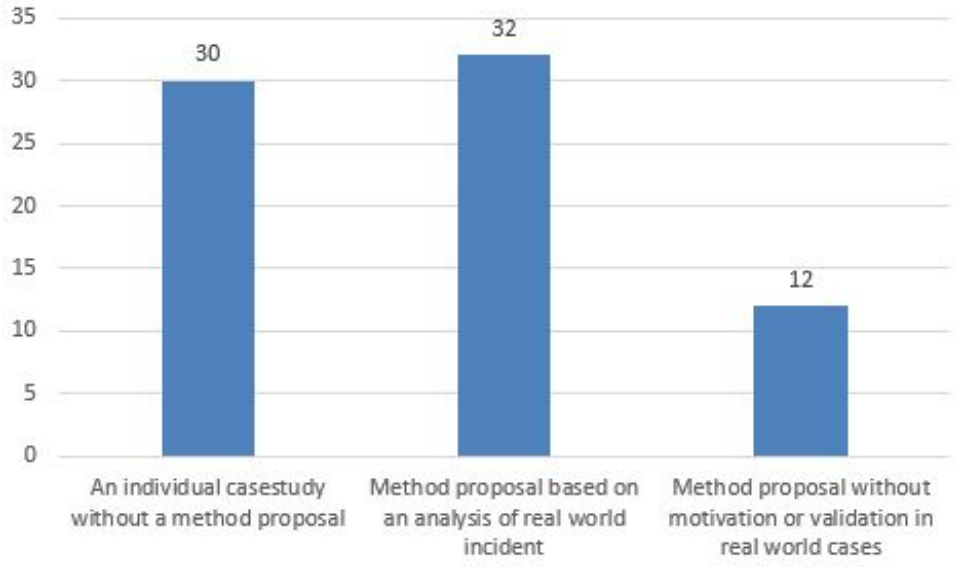

Figure 5: Number of method proposals, case studies, and combinations of those

	amp; **Risk Assessment**	amp; **Incident Reporting**
Telecommunication domain	amp; 23	amp; 21
Non-telecommunication domain	amp; 18	amp; 17

Table 1: Classification of studies according to domain.

1. Study of risk assessment only (39 papers).
2. Study of incident analysis only (35 papers).
3. Study of risk assessment and incident analysis (5 papers).

In table 1, we split these categories according to the domain.

For example, Wojtasik & Skoglund study shows how the selection of power solutions, cost, and risk factors may trigger incidents with varying intensity (Wojtasik and Skoglund, 2003). This is an example of a study of type (1).

Morrison discusses the Network Disaster Recovery (NDR) system of the AT&T network, which is responsible for response processes to maintain communication (Morrison, 2011). This is an example of a study of type 2. George et al. discussed offer a comprehensive understanding of cybercrime incidents and resolution guidelines (Tsakalidis and Vergidis, 2017). Identified features of cybercrime incidents are risk-based and provided schema is a step toward resolution of the incident.

Table 1 shows that only 21 studies report about incidents in the telecom domain. This is a small fraction of the total number of telecom incidents that have occurred in the period 1990-2017. For example, ENISA reported a total of 158 incidents in Europe in the year 2016 only. A number of incidents reported by ENISA can be traced to reports in social media but not to reports in the scientific literature (Van Eeten et al., 2011).

A plausible explanation of the low number of published telecom incident analysis studies is that incident analyses are highly confidential.

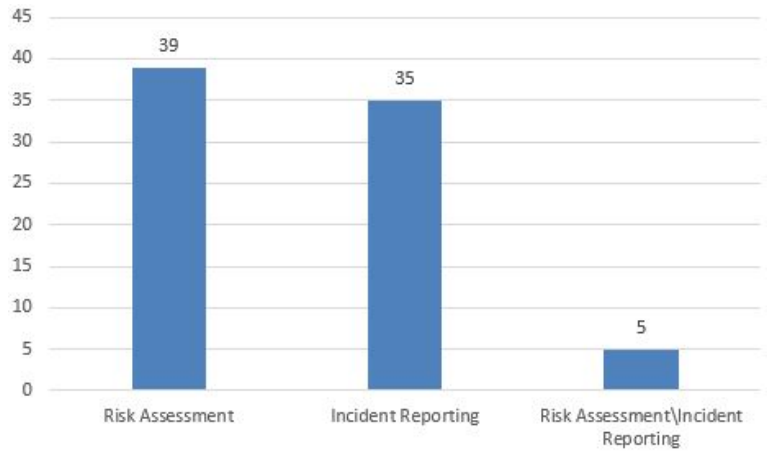

Figure 6: Classification of studies into those focussing on risk assessment and on incident reporting. Five studies focus on both.

To sum up, our findings of RQ1, very few telecom incidents have been reported in the scientific literature, probably due to confidentiality constraints. Almost all scientific interest goes to the definition of methods, with or without motivation in real-world case studies. About half of the method focuses on incident analysis. The others focus on risk assessment. There are no papers that validate a scientific proposal of a method.

Our preliminary conclusions are that there is a need for real-world validations of incident analysis method proposals.

3.2 RQ2 What incident analysis methods have been used?

Sr.	Reference	Method
1	(Bonhomme et al., 2010)	Multi-Agent System reaction architecture
2	(Carrillo and Chamorro, 2014)	eSUPERTEL
3	(Doytchev and Szwillus, 2009)	Fault Tree Analysis (FTA) and Task Analysis (TA)
4	(Fraisse and Buchsbaum, 2002)	high availability, high quality power architecture
5	(Gâteau et al., 2009)	Multi-agents based Architecture,
6	(Jaeger et al., 2007)	Community Response Grid
7	(Kwasinski et al., 2009)	Fault tree analysis
8	(Lindman and Thorsell, 1996)	Distributed power models i.e mathematical optimization based
9	(Luna et al., 2008)	GrEA- Mathematical
10	(Paolino et al., 2011)	MASF MODEL
11	(Roos, 2002)	Incident analysis based on techniques SPAT, Olsen
12	(Zaman et al., 2015)	E-stream
13	(Choi et al., 2016)	Network forensics system
14	(Fagade et al., 2017)	System Dynamic approach
15	(Bloomfield et al., 2017)	Interdependency Analysis
16	(Hu et al., 2017)	Rule based telecom Monitoring
17	(Salah et al., 2018)	Architecture
18	(Ordóñez et al., 2016)	AUTO framework
19	(Hiran et al., 2013)	Control/Data-Plane measurements
20	(Frommholz et al., 2016)	PEN
21	(Gai et al., 2016)	Cost-Aware Hierarchical Cyber Incident Analytics (CA-HCIA) Framework
22	(Hung et al., 2006)	Data mining

Sr.	Reference	Method
23	(Patricelli et al., 2009)	NGN layered Architecture, MOBSAT
24	(Salmon et al., 2014)	Accimap
25	(Tsakalidis and Vergidis, 2017)	Incident description Schema

Table 2: Methods and Approaches mentioned in literature

Appendix B summarizes the 74 reviewed papers in table form. Table 2 lists the methods described in the papers.Table 3 lists the papers in the different categories, and also splits the found methods in telecom and non-telecom-oriented papers. Detailed descriptions of these methods are provided in Appendix C and D. In Figure 7, we have classified the methods according to the stage of incident analysis and in Figure 8 according to the aspect of the system where the incident occurred. For the post-incident analysis methods, we used the classification of Avižienis et al. (Avizienis et al., 2004), where after *error detection* there is *recovery* to a state without the detected errors and without faults that can be activated again.

Independently of this, in Figure 8 we distinguish methods that focus on technical or organizational aspects of the incident, or on elements external to the organization responsible for the system where the incident occurred.

We next describe some methods to illustrate the different categories.

1. **Pre-incident methods.** Pre-incident methods typically address an aspect of risk management, which consists of a continual process of risk monitoring and control, and a periodic process of risk assessment. Risk assessment, in turn, consists of risk identification, analysis, evaluation, and mitigation. More than half of the 34 analysis methods that we found are pre-incident methods. Three of those review potential risks associated with a particular event or action. For example, Hu et al. describe a method for rule-based cyber-security incident monitoring (Hu et al., 2017). Bloomfield et al. proposed an interdependency risk analysis in critical infrastructures such as the telecommunication infrastructure (Bloomfield et al., 2017). Fagade et al. provide a high-level threat modeling process by considering personality risk indicators, behavior risk indicators, and technical risk indicators (Fagade et al., 2017). Salmon et al. identified that human factors have a crucial role to play in examining and enhancing systems (Salmon et al., 2014). They utilized the incident analysis method AcciMap to identify human factors in disaster response (Branford et al., 2009).

   The following methods focus on one of the aspects of telecom incident risk management.

   (a) **Pre-incident methods: Technical Aspects**

   Telecommunication systems depend on power systems, and several risk analysis methods focus on the power supply. Some examples are the work of Lindman & Thorsell proposes increasing reliability by distributed ac/dc power modules (Lindman and Thorsell, 1996). This also facilitates live insertion of power modules without interrupting service. And Stojmenovic et al. propose the use of power cost metrics and power-aware routing algorithm to minimize the total power needed to route a message between a source and a destination (Stojmenovic and Lin, 2001). Moreover, Fraisse & Buchsbaum proposes power plant architectures that increase the availability of the system (Fraisse and Buchsbaum, 2002).

   Frommhol et al. are the only ones not discussing power supply (Frommholz et al., 2016). They propose the use of information retrieval and machine learning techniques to predict and detect cyberattacks.

   (b) **Pre-incident methods: Organizational aspects** Organizational factors play a big role during and after an incident. There exist a considerable amount of literature about organizational factors involved. Organizational policies, management interests, and culture are key impact factors before, during, and after an incident, and several papers focus on these. Bonhomme et al. (Bonhomme et al., 2010), Paolino et al. (Paolino et al., 2011) and Gâteau et al. (Gâteau et al., 2009) all describe multi-agent systems that detect or report incidents. We classify these as pre-incident

	amp; **(1) Methods proposed, No motivation nor validation**	amp; **(2) Motivational case study, method proposed, no validation**	amp; **(3) Case study, no method proposed**
Telecommunication	amp; Incident description Schema (Tsakalidis and Vergidis, 2017) Cost-Aware Hierarchical Cyber Incident Analytics (CA-HCIA) Framework (Gai et al., 2016) ,Data mining (Hung et al., 2006), PEN (Frommholz et al., 2016), Multi-Agent System reaction architecture(Bonhomme et al., 2010), Community Response Grid(Jaeger et al., 2007), GrEA- Mathematical (Luna et al., 2008), MASF MODEL (Paolino et al., 2011),	amp; NGN layered Architecture, MOBSAT (Patricelli et al., 2009), Control/Data-Plane measurements(Hiran et al., 2013) ,E-Stream (Zaman et al., 2015), Network forensics system (Choi et al., 2016), Interdependency Analysis (Bloomfield et al., 2017), Rule based telecom Monitoring (Hu et al., 2017), Architecture (Salah et al., 2018)	amp; eSUPERTEL (Carrillo and Chamorro, 2014),
No Telecommunication	amp; Multi-agents based Architecture(Gâteau et al., 2009),Distributed power models (Lindman and Thorsell, 1996) , System Dynamic approach (Fagade et al., 2017) , AUTO framework (Ordóñez et al., 2016)	amp; Incident analysis based on techniques SPAT(Roos, 2002) , Fault tree (Doytchev and Szwillus, 2009) (Kwasinski et al., 2009) , high availability high quality power architecture (Fraisse and Buchsbaum, 2002), Accimap (Salmon et al., 2014)	amp; None

Table 3: Lack of motivation and validation of proposed methods in the telecom and non-telecom domains.

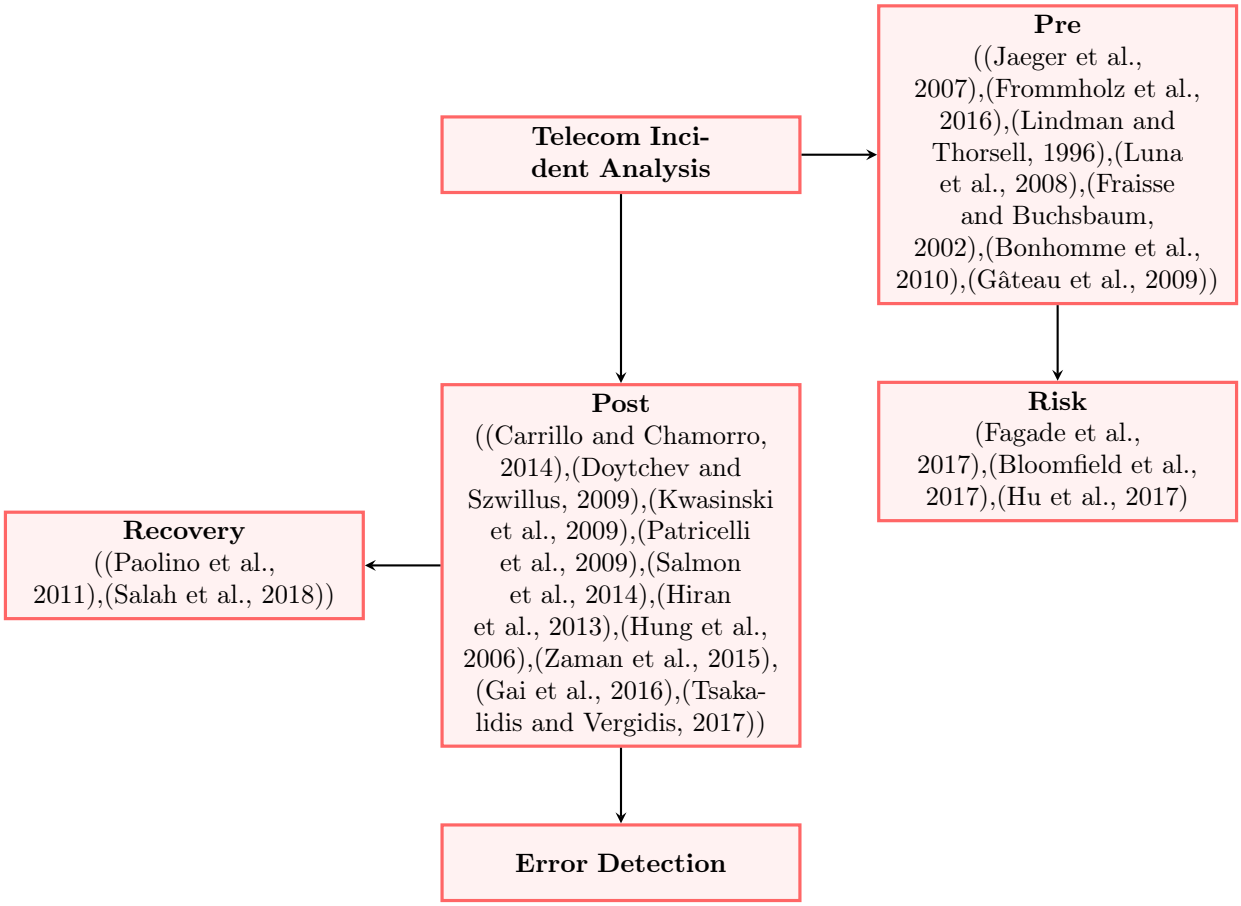

Figure 7: Taxonomy of Incident Analysis according to the analysis stage. The arrows point to subclasses.

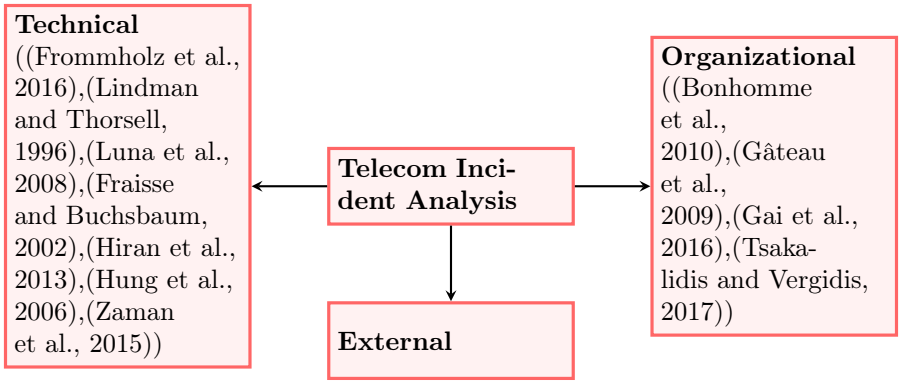

Figure 8: Taxonomy of Incident Analysis according to analyzed aspect. The arrows point to subclasses.

methods because these systems should be installed before an incident happens. They do not provide guidelines for incident analysis.

2. **Post Incident methods** A number of methods are neutral for a focus on technical or organizational aspects, and with respect to error detection or recovery. For example, fault tree analysis and task analysis are both used in the incident analysis but are neutral concerning these aspects and analysis tasks. Doytchev & Szwillus use a combination of the two: Fault tree analysis is used to identify the root causes of an incident, and task analysis to analyze the interaction between people and their environment (Doytchev and Szwillus, 2009). This was applied in a case study of an incident in a Bulgarian Hydropower plant. Task analysis helped to find out which tasks have been performed and which have been omitted. Kwasinski et al. also showed that task analysis can help to identify behavioral causes of an incident (Kwasinski et al., 2009).

   Patricelli et al. proposed a technique that can be used to analyze incidents where telecommunication platforms become non-available due to a disaster (Patricelli et al., 2009). The MOBSAT unit they propose is a mobile telecommunications unit that can be used to communicate between the disaster site and the support centers.

   A number of papers focused on the recovery task and the technical and organizational aspects, respectively.

   (a) **Post Incident Methods: Recovery**

   The paper by Paolino et al. mentioned above, proposes an agent-based system for decision support that must be installed pre-incident and is used post-incident. So we may additionally classify it as a post-incident method with a focus on the recovery task (Paolino et al., 2011).

   Salah et al. propose an information ticketing system to support the incident resolution process (Salah et al., 2018). A ticket is the formal registration of an incident. Using a dataset from a vast telecommunications network, they provide evidence that using tickets can accelerate the incident resolution process.

   (b) **Post Incident methods: Technical** Hiran et al. present a case study of an incident in which a telecom system was hijacked (Hiran et al., 2013). The paper presents the root cause analysis of the incident.

   (c) **Post Incident methods: Organizational aspect** Many methods focus on the organizational aspect of incident analysis.

   Aas defines the Human Factors Assessment and Classification System (HFACS), which classifies human errors with major accident potential (Aas, 2009). Empirical evidence showed that almost three-quarters of all causal factors in incidents are due to unsafe human acts.

   Later the method was refined with a distinction between active and latent failures, by which they measure failures with immediate or delayed effect (Shappell and Wiegmann, 2012). This distinction was later used by Reason in his Swiss Cheese Model of accident causation (Shappell and Wiegmann, 2012).

   An extension of HFACS is Chen & Chou (Chen and Chou, 2012) where Reason's Generic Error Modelling System (GEMS) and Hawkins's SHEL model (Molloy and O'Boyle, 2005) and applied it to maritime systems.

   Roos analyzed human factors from the customer perspective. Roos (Roos, 2002) defines Switching Path Analysis Technique (SPAT) to identify customers that switched to another service provider after a significant incident.

   Ordóñez et al. (Ordóñez et al., 2015; Ordóñez et al., 2016) propose the AUTO framework for monitoring automatic reconfiguration of telecommunication service composition. AUTO uses semantic technologies and ITIL.

   Choi et al. (Choi et al., 2016) take the cybersecurity perspective and designed CyberBlackbox, a network forensics system that analyzes network traffic to look for possible attacks. Tsakalidis

& Vergidis (Tsakalidis and Vergidis, 2017) provide a classification of cyber-crime incidents that can be used in cyber-crimes incidents identification and analysis from an organizational perspective. Gai et al. (Gai et al., 2016) take a very different point of view and introduce the concept of Cybersecurity Insurance to cover the damage caused by an incident.

Two methods in the reviewed literature do not fall in the taxonomy of Figure 13. eSUPERTEL (Carrillo and Chamorro, 2014) and E-stream (Chaparadza, 2009) define incident *reporting* methods and are outside the scope of this paper.

To sum up our findings of RQ2, there is no evidence that the methods proposed by research are actually used in practice.

We conclude from our findings of RQ2 that there is a need for methods that include both technical and organizational aspects and provide support for both stages of error recovery.

3.3 RQ3 Root causes of telecom incidents

Root cause identification is the first step of incident analysis (Lekberg, 1997). Many analysis methods distinguish between initial and detailed root causes. ENISA defines initial root cause as the event that triggered the incident and detailed root cause as an event or chain of events that subsequently played a role in the incident (European Union Agency For Network And Information Security, 2017). Root cause categories give a broader summary of the most common types of incidents. In the following we will highlight root cause categories in a set of more detailed causes.According to ENISA (European Union Agency For Network And Information Security, 2017)

"An incident is often a chain of events and failures, involving multiple causes. For instance, an incident may be triggered by storm, heavy winds, which tear down power supply infrastructure, then cause a power cut, which in turn leads to an outage because base stations are without power. For this incident both heavy winds and power cuts are listed as detailed causes. In the annual summary reporting ENISA keep track of these detailed causes."

Scientific literature also supports ENISA's description of initial and detailed root cause. As an example, Kwasinski et al.(Kwasinski et al., 2009) discuss the impact of Hurricane Katrina in October 2005 on the telecommunications power infrastructure. The study revealed that system failure was due to lack of power supply to the central network elements. This in turn was caused by fuel supply disruptions, flooding, and security breaches. Power supply disruption of the central network elements is then the initial root cause, and the factors that caused power supply disruption are the detailed root causes. ENISA have used four division for initial root cause identification as shown from the Figure 9 initial root cause identification based on ENISA reports from 2013-2017, literature shows that there are many other root causes of an incident, such as power failure and network failure that contribute to incidents occurrence. ENISA uses a less detailed classification (Dekker et al., 2011) However we have introduced an "unknown" division in the initial root cause categorization as can be seen from Figure 10 where we applied ENISA's classification to the literature.

The reviewed 74 papers listed a total of 63 detailed root causes, which we classified in 15 different initial root causes, shown in Figure 11. The most frequent known cause is network failure, followed by power failure. Figure 11 thus shows a more detailed subdivision of ENISA's system failures class.

- **System failures** – this is the largest category and includes incidents caused by failure of hardware or software.
- **Human errors** – includes incidents caused by errors committed by employees/people involved in the successful delivery of the service. Figure 11. has a human error class too.
- **Malicious actions** – includes incidents due to an attack, e.g a cyberattack or a cable theft. This corresponds to the cybersecurity incident in Figure 11.
- **Natural phenomena** –includes incidents caused by natural disasters such as storms, floods, heavy snowfall, and earthquakes. This corresponds to the disaster class in Figure 11.

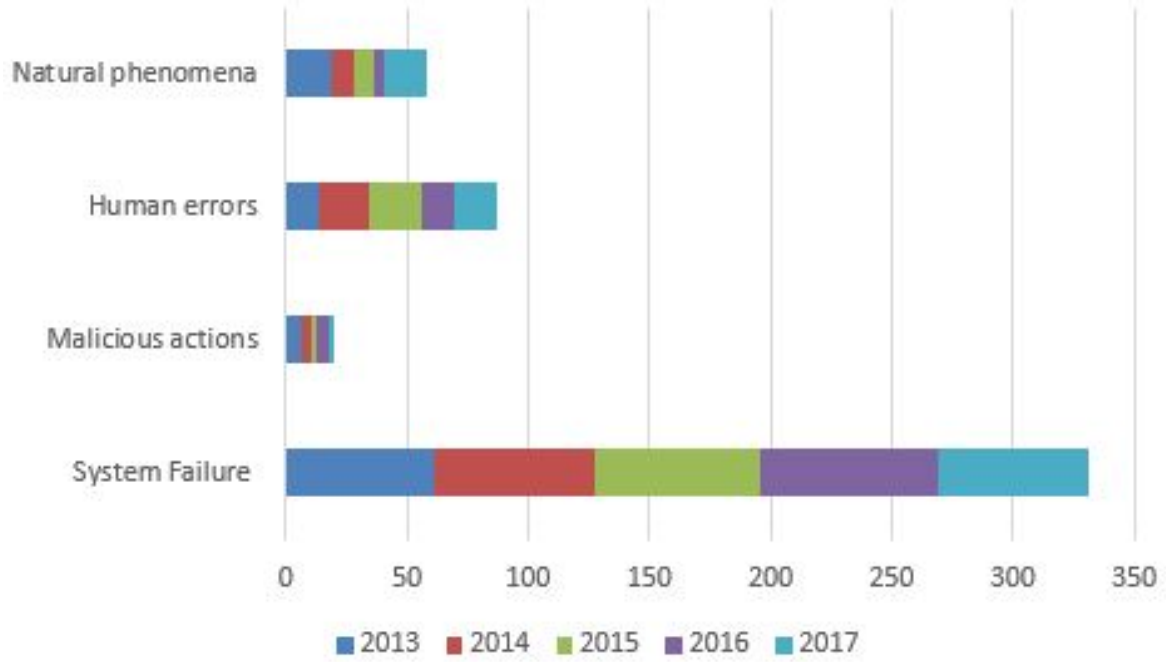

Figure 9: Initial root cause identification based on ENISA report 2013-2017

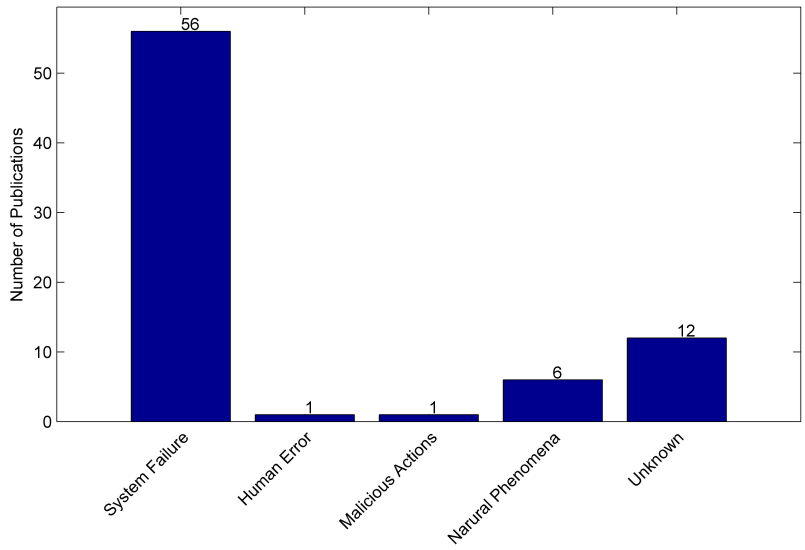

Figure 10: Initial Root cause identification based on ENISA standard

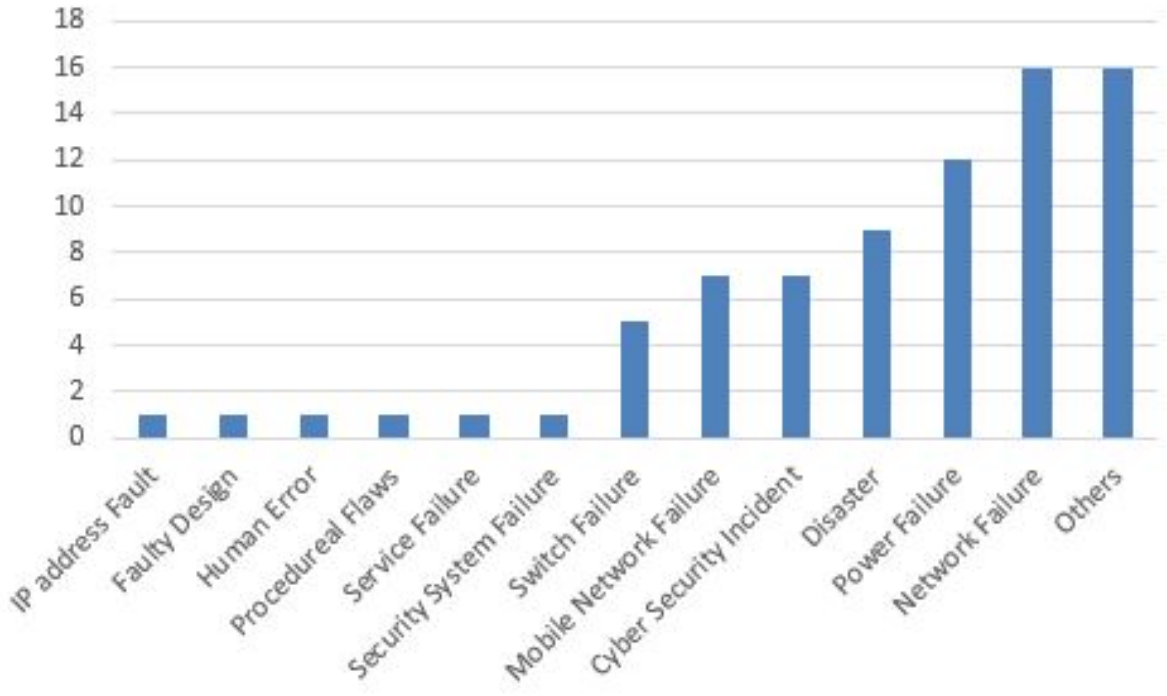

Figure 11: Classification of root causes found in the literature

In their yearly reports, ENISA uses a more detailed classification, just as we do, but their detailed classification changes from year to year (European Union Agency For Network And Information Security, 2014; European Union Agency For Network And Information Security, 2015; European Union Agency For Network And Information Security, 2016; European Union Agency For Network And Information Security, 2017). A summary of ENISA's identified causes is provided in Figure 12 Comparison of this detail classification with our classification of root causes found the literature (Figure 11) reveals that there is very little overlap between the two classifications. This may be a consequence of the small sample of incidents that are considered in the literature compared to the wide variety of incidents that occur in the large sample of real-world incidents in ENISA's databases.

A second observation to be made about these root cause classifications is that they are very detailed regarding technical causes but provide little information about possible organizational causes.

Third, there is an unbalanced classification of internal causes versus external causes. Internal causes occur in the telecom system being investigated. They are the technical failures and human errors in the ENISA classification. External causes occur in the environment of the system. These are classified as malicious actions and natural phenomena in the ENISA classification. It is puzzling that there are no technical failures or human errors *outside* the system being evaluated, that contributed to the incident.

To sum up our findings about RQ3, the majority of incidents reported in the literature are system failures of a wide variety of kinds. A small number are human errors. Malicious actions and natural phenomena are more prominent in the reviewed literature than they are in the yearly ENISA reports. These differences may be due to small sample size of the incidents reviewed in the literature.

Our analysis of the literature and of the ENISA reports reveal that most reported causes are technical. It is an open question whether this is due to a technical focus of the methods used for analyses, or due to the fact that most root causes were in fact technical (and not organizational). Our preliminary conclusion is that any new method to be proposed for telecom incident analysis must keep a balance between technical and organizational causes, and between internal and external causes.

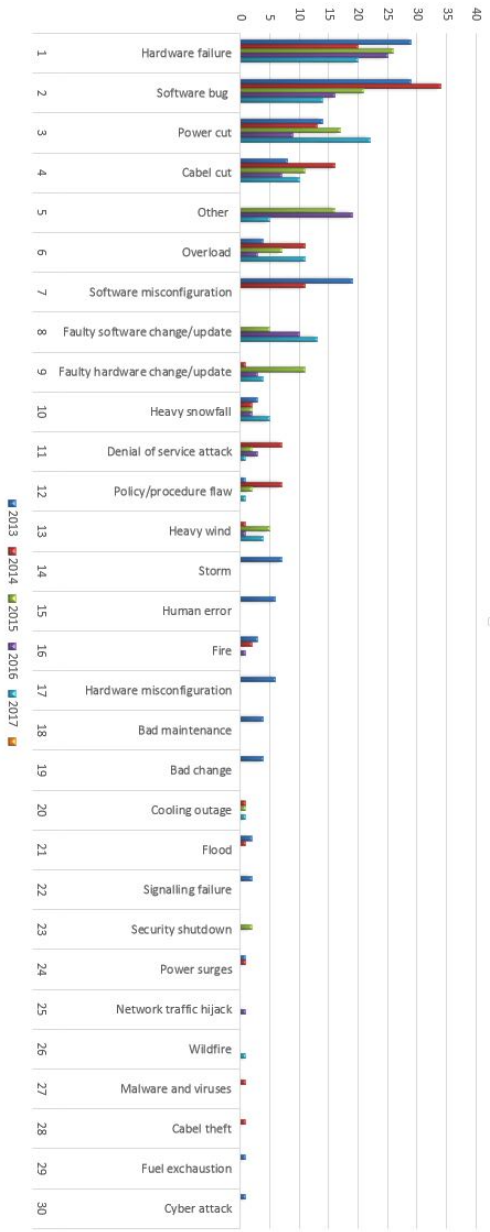

Figure 12: Subsequent root cause identification based on ENISA report 2013-2017

4 Discussion

4.1 Answers to research questions

We now summarize the answers to our research questions.

- **RQ1:** What telecom incidents have been reported in the scientific literature?

  There are very few scientific reports of real-world telecommunication incidents. This is probably due to confidentiality constraints. Almost all scientific interest goes to the definition of methods. However, there are no published reports of method validations in practice. We conclude that there is lack of real-world validations of incident analysis method proposals, and for scientific reports about this that respect confidentiality constraints.

- **RQ2:** What incident analysis methods have been used?

  There is no evidence that the methods proposed by research are actually used in practice. Two practical methods that are widely used are fault tree analysis and task analysis. All methods focus either on technical or on organizational aspects of the incident. Moreover, they focus more on error detection than on error recovery. We conclude that there is a need for methods that include both technical and organizational aspects, and provide more support for error recovery.

- **RQ3:** What root causes of telecom incidents have been reported?

  The majority of incidents reported in the literature are system failures of a wide variety of kinds. A small number are human errors. There is a wide variety of kinds of root causes both in the scientific literature and in the yearly ENISA reports. The category of technical internal causes is heavily populated compared to the other root cause categories. We conclude that any new method to be proposed for telecom incident analysis must keep a balance between technical and organizational causes, and between internal and external causes.

4.2 Limitations to validity

The major threat to validity is the possibility of incompleteness of the reviewed literature list. There is no uniformly accepted unambiguous set of terms to describe incidents and accidents, and this may have caused us to miss relevant literature. We tried to mitigate this threat by varying our keywords in the search string. In addition, we included a paper if it satisfied only three out of our four inclusion criteria. So we cast the net as widely as possible.

However, we restricted our search to English- and Dutch-language reports, and this too may have caused us to miss some relevant literature too.

We tested the validity of our result by periodically asking feedback from experts in the telecom field, who gave their opinion about the intermediary results.

4.3 Conclusion and Future work

Our conclusion from this survey is that there is no need for yet another academic proposal for an incident analysis method, but for real-world validations of existing methods. At the same time, existing methods may need adaptation to redress the balance between attention for technical and organizational causes, and between attention for internal and external causes.

In line with this, we have applied the ACCIMAP method to a real-world incident analysis and updated it based on our experience and the conclusions of this literature review. We are currently applying the updated methods, T-Accimap, to two new cases and have formulated guidelines for improving the structure of incident reports to facilitate lessons learned that preserve confidentiality.

APPENDICES

A Data Extraction from Literature for Research Question 1

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
1	Zaman F., Hogan G., Der Meer S., Keeney J., Robitzsch S., Muntean G.-	A recommender system architecture for predictive telecom network management	2015	IEEE Communications Magazine		Dublin City University, Ireland; Centre for Global Intelligent Content, Ireland; Department of Ericsson, Ireland		Article
2	Eldh S., Punnekkat S., Hansson H., Jonsson	Component testing is not Enough - A study of software faults in telecom middleware	2007	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	5	Ericsson AB, Kistagången 26, Stockholm, Sweden; Malardalens University, Ericsson AB, Kistagangen 26, Stockholm, Sweden; Combitech., Ericsson AB, Kistagangen 26, Stockholm, Sweden	Fault classification; Fault distribution; Software; Testing	Conference Paper
3	"Lindman P., Thorsell L.(Lindman and Thorsell, 1996)	Applying distributed power modules in telecom systems	1996	IEEE Transactions on Power Electronics	22	IEEE; Ericsson Components AB, Energy Systems Division, S-164 81 Kista-Stockholm, Sweden		Article
4	Hiran R., Carlsson N., Gill P.(Hiran et al., 2013)	Characterizing large-scale routing anomalies: A case study of the China telecom incident	2013	Lecture Notes in Computer Science	1	Linkoping University, Sweden; Citizen Lab, Munk School of Global Affairs, University of Toronto, Canada	Border Gateway Protocol; Measurement; Routing; Security	Conference Paper
5	Doytchev D.E. , Szwillus.(Doytchev and Szwillus, 2009)	Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria	2009	Accident Analysis and Prevention	22	Faculty of Computer Science, Electrical Engineering and Mathematics, University of Paderborn, 33102 Paderborn, Germany	Fault tree analysis; Human error identification; Incident analysis; Performance shaping factors; Task analysis	Article
6	Jaeger P.T., Shneiderman B., Fleischmann K.R., Preece J., Qu Y., Fei Wu P.(Jaeger et al., 2007)	Community response grids: E-government, social networks, and effective emergency management	2007	Telecommunications Policy	66	College of Information Studies, University of Maryland, 4105J Hornbake Building, College Park, 20742-4345 MD, United States; Department of Computer Science, University of Maryland, MD, United States	Community response grid; E-government; Emergency response; Mobile communications; Public policy; Social networks	Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
7	Anderson, Peter S(Anderson, 2002)	Critical infrastructure protection in the information age	2002	DUP Science, Delft	10			Policy
8	Steenbruggen J., Borzacchiello M.T., Nijkamp P., Scholten H.(Steenbruggen et al., 2013)	Data from telecommunication networks for incident management: An exploratory review on transport safety and security	2013	Transport Policy	9	VU University, Department of Spatial Economics, De Boelelaan 1105, 1081 HV Amsterdam, Netherlands; Joint Research Centre, Institute for Environment and Sustainability, Digital Earth and Reference Data Unit, Via Enrico Fermi, 2749-T.P. 262, I-21027 Ispra (VA), Italy	Incident management (IM); Mobile phones; Situation awareness; Telecommunication network; Transport safety; Transport security	Article
9	Patricelli F., Beakley J.E., Carnevale A., Tarabochia M., von Lubitz D.K.J.E.(Patricelli et al., 2009)	Disaster management and mitigation: The telecommunications infrastructure	2009	Disasters	17	Zain (formerly MTC) Head Offices, Seef District, Bahrain; LJT and Associates, US Navy Anti-Terrorism Force Protection Program, San Diego, CA, United States; Volontari Abruzzesi per la Protezione Civile, L'Aquila, Italy; BIP ITALIA Ltd., Caporciano, Italy; H.G. and G.A. Dow College of Health Sciences, Central Michigan University, Mt. Pleasant, MI 48804, United States; MedSMART, Inc., Ann Arbor, MI 48904, United States	Disaster management; Mobile and satellite telecommunications; Network Enabled Capability; Network-centricity; Next Generation Network	Article
10	Pace P., Aloi G.(Pace and Aloi, 2008)	Disaster monitoring and mitigation using aerospace technologies and integrated telecommunication networks	2008	IEEE Aerospace and Electronic Systems Magazine	21	University of Calabria		Article
11	Samarajiva, Rohan (Samarajiva, 2001)	Disaster-preparedness and recovery: a priority for telecom regulatory agencies in liberalized environments	2001	International Journal of Regulation and Governance	6	LIRNE.NET, Economics of Infrastructures Section, Faculty of Technology, Policy, and Management, Delft University of Technology, The Netherlands		Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
12	Fraisse, Michel and Buchsbaum, Laurent (Fraisse and Buchsbaum, 2002)	Environment friendly high quality, high availability telecom power plant architecture	2002	Telecommunications Energy Conference, 2002. INTELEC. 24th Annual International	11	MGE UPS SYSTEMS, St. Ismier, France		Conference Paper
13	Townsend, Anthony M and Moss, Mitchell L (Townsend and Moss, 2005)	Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communication	2005	Robert F. Wagner Graduate School of Public Service, New York University	43	Robert F. Wagner Graduate School of Public Service, New York University		Technical Report
14	Katsakiori P., Sakellaropoulos G., Manatakis E.(Katsakiori et al., 2009)	Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models	2009	Safety Science	52	Department of Mechanical Engineering and Aeronautics, University of Patras, 26 504 Rion, Greece; Department of Medical Physics, School of Medicine, University of Patras, Greece	Accident causation models; Accident investigation methods	Article
15	Seung-June Yi, Sung-Jun Park, Young-dae Lee, Sung-Duck Chun (Yi et al., 2012)	Method for detecting security error in mobile telecommunications system and device of mobile telecommunications	2008	Patent Office	25	LG Electronics Inc.		Patent
16	Arthur B. Williams, David T. Lundquist (Williams and Lundquist, 1993).	Method for remote power fail detection and maintaining continuous operation for data and voice devices operating over local loops	1993	Patent Office	94	Coherent Communications Systems Corp.		Patent
17	Dien Y., Llory M., Montmayeul(Dien et al., 2004)	Organisational accidents investigation methodology and lessons learned	2004	Journal of Hazardous Materials	35	Department MRI, Electricite de France, Recherche et Developpement, 1 Avenue du General de Gavlle, Clamart 92140, France; Institut du Travail Humain, 17 Rue des Espessas, Gallargues le Montueux, 30660, France	Accident analysis methods; Organisational accidents; Organisational incidents	Conference Paper
18	Grover W.D., Venables B.D., Sandham J.H., Milne A.F.(Grover et al., 1990)	Performance studies of a selfhealing network protocol in Telecom Canada long haul networks	1990	IEEE Global Telecommunications Conference and Exhibition	2	Alberta Telecommun Res Centre,, Edmonton, Alta, Canada		Conference Paper

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
19	"Stojmenovic I., Lin X. (Stojmenovic and Lin, 2001)	Power-aware localized routing in wireless networks	2001	IEEE Transactions on Parallel and Distributed Systems	425	DISCA, IIMAS, UNAM, Ciudad Universitaria, Coyoacan, Mexico DF 04510, Mexico; SITE, University of Ottawa, Ont., KIN 6N5, Canada; Cognos Inc., 3755 Riverside Drive, Ottawa, ON, K1G 4K9, Canada	Distributed algorithms; Power management; Routing; Wireless networks	Article
20	Mockler, Robert J (Mockler, 2003)	Prescription for disaster: failure to balance structured and unstructured thinking	2003	Business Strategy Review	21	St John's University's Graduate Business Program, Tobin College of Business		Article
21	Herrlin M(Herrlin et al., 2005)	Rack cooling effectiveness in data centers and telecom central offices: The Rack Cooling Index (RCI)	2005	ASHRAE Transactions	42	ASHRAE, United States; ANCIS Incorporated, San Francisco, CA, United States		Conference Paper
22	Morrison K.(Morrison, 2011)	Rapidly recovering from the catastrophic loss of a major telecommunications office	2011	IEEE Communications Magazine	19	AT and T, United States		Conference Paper
23	Pirzada A.A., Portmann M., Wishart R., Indulska J.(Pirzada et al., 2009)	SafeMesh: A wireless mesh network routing protocol for incident area communications	2009	Pervasive and Mobile Computing	14	Queensland Research Laboratory, NICTA, Brisbane, QLD 4072, Australia; School of ITEE, The University of Queensland, Brisbane, QLD 4072, Australia	Crisis management; Incident area communications; Wireless mesh network	Article
24	Luna F., Nebro A.J., Alba E., Durillo J.J.(Luna et al., 2008)	Solving large-scale real-world telecommunication problems using a grid-based genetic algorithm	2008	Engineering Optimization	15	Departamento de Lenguajes y Ciencias de la Computación, Universidad de Málaga, Málaga, Spain	Frequency assignment problem; Genetic algorithms; Grid computing; Real-world problem solving	Article
25	Juan A. Paz Salgado, Jose Manuel Montero Duran, Jose Maria Rey Poza, Mario Lopez Gallego (Salgado et al., 2013)	System and method of diagnosis of incidents and technical support regarding communication services	2013	Patent Office	4	Telefonica, S.A.		Patent

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
26	Salah, Saeed and Maciá-Fernández, Gabriel and Díaz-Verdejo, Jesús E (Salah et al., 2018)	Fusing Information from Tickets and Alerts to Improve the Incident Resolution Process	2018	Information Fusion	0	Department of Signal Theory, Telematics and Communications - CITIC, University of Granada, c/ Periodista Daniel Saucedo Aranda, s/n Granada 18071, Spain	Quality of service, Data analysis, Network management systems, Alert correlation, Ticket-alert correlation	Article
27	Redl, Richard and Kislovski, Andre S (Redl and Kislovski, 1995)	Telecom power supplies and power quality	1995	Telecommunications Energy Conference, 1995. INTELEC'95., 17th International	38	ELFI SA, Onnens, Switzerland		Conference Paper
28	Kwasinski A., Weaver W.W., Chapman P.L., Krein P.T.(Kwasinski et al., 2009)	Telecommunications power plant damage assessment for hurricane katrina-site survey and follow-up results	2009	IEEE Systems Journal	31	Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78729, United States; Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931, United States; Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801, United States	Damage assessment; Hurricane; Natural disaster; Power systems; Telecommunications power	Article
29	Van Eeten M., Nieuwenhuijs A., Luiijf E., Klaver M., Cruz E.(Van Eeten et al., 2011)	The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports	2011	Public Administration	24	The Faculty of Technology, Policy and Management, Delft University of Technology, Netherlands; Albert Nieuwenhuijs, TNO (Defence, Security and Safety), The Hague, Netherlands		Article
30	Fabian B., Baumann A., Lackner(Fabian et al., 2015)	Topological analysis of cloud service connectivity	2015	Computers and Industrial Engineering	1	Institute of Information Systems, Humboldt-Universitat zu Berlin, Spandauer Str. 1, Berlin, Germany	Availability; Cloud computing; Complex networks; Connectivity	Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
31	Goldiner, Andrey and Golovko, Vladimir and Ljubelskiy, Aleksey (Goldiner et al., 2000)	Uninterruptible power supply system for powering of telecom equipment	2000	Telecommunications Energy Special Conference, 2000. TELESCON 2000. The Third International	1	Electrosystems Ltd., St. Petersburg, Russia		Conference Paper
32	Paolino L., Paggi H., Alonso F., Lopez G. (Paolino et al., 2011)	Solving incidents in telecommunications using a multi-agent system	2011	Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, ISI 2011	1	Facultad de Ingeniera, Universidad ORT Uruguay, Montevideo, Uruguay; Facultad de Informatica, Universidad Politcnica de Madrid, Spain	incident; multi-agent system; severities; subject of an incident	Conference Paper
33	Ordonez A., Eraso L., Falcarin P.(Ordóñez et al., 2015)	Rule-based monitoring and error detecting for converged telecommunication processes	2015	IntelliSys 2015 - Proceedings of 2015 SAI Intelligent Systems Conference	0	Intelligent Mangement System Group, University Foundation of Popayán, Popayán, CO, Colombia; School of Architecture, Computing and Engineering, University of East London, London, United Kingdom	automated planning; automated reconfiguration; convergent services; service composition; Service monitoring	Conference Paper
34	Ovcjak B., Hericko M., Polancic G.(Ovčjak et al., 2015)	Factors impacting the acceptance of mobile data services - A systematic literature review	2015	Computers in Human Behavior	2	Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia	Acceptance models; Mobile data services; Mobile service categories; Systematic literature review; Technology acceptance	Article
35	Carrillo B., Chamorro S.(Carrillo and Chamorro, 2014)	Mobile system of recording incidents in telecommunications services: ESUPERTEL	2014	2014 1st International Conference on eDemocracy and eGovernment, ICEDEG 2014	0	Superintendence of Telecommunications (SUPERTEL), Ecuador	mobile system; requirement input channels; SM-RIT; SUPERTEL; telecommunications users	Conference Paper
36	Luo Z., Li K., Ma X., Zhou J.(Luo et al., 2013)	A new accident analysis method based on complex network and cascading failure	2013	Discrete Dynamics in Nature and Society	2	State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China		Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
37	Chen S.-T., Chou Y.-H.(Chen and Chou, 2012)	Examining human factors for marine casualties using HFACS - Maritime accidents (HFACS-MA)	2012	2012 12th International Conference on ITS Telecommunications, ITST 2012	1	Merchant Marine Department, National Taiwan Ocean University, Keelung, Taiwan	Accident analysis; HFACS; Human factors; Why-Because Analysis	Conference Paper
38	Bonhomme C., Feltus C., Khadraoui D.(Bonhomme et al., 2010)	A multi-agent based decision mechanism for incident reaction in telecommunication network	2010	2010 ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2010	1	Public Research Centre Henri Tudor, 29, Avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg	Bayesian network; Decision system; Distributed network; Multi-agents system; Reaction; Security	Conference Paper
39	Gateau B., Khadraoui D., Feltus C.(Gâteau et al., 2009)	Multi-agents system service based platform in telecommunication security incident reaction	2009	2009 Global Information Infrastructure Symposium, GIIS '09	0	Centre for IT Innovation, Public Research Centre Henri Tudor, 29, Avenue John F. Kennedy, L-1855 Luxemburg, Luxembourg	Architecture; Distributed networks; Multi-agents systems; Security policy	Conference Paper
40	Aas A.L.(Aas, 2009)	Probing human error as causal factor in incidents with major accident potential	2009	Proceedings of the 3rd International Conference on Digital Society, ICDS 2009	1	Dept. of Computer and Information Science, Norwegian University of Science and Technology (NTNU), Sem Saelands vei 7-9, NO-7491 Trondheim, Norway		Conference Paper
41	Shi T., Zhao J., Yin X., Wang J.(Shi et al., 2008)	Research on telecommunication switching system survivability based on stochastic petri net	2008	3rd International Conference on Innovative Computing Information and Control, ICICIC'08	0	Department of Computer Science and Engineering, College of Information Engineering, Yangzhou University, Yangzhou Jiangsu, 225009, China		Conference Paper
42	Song L., Zhang J., Mukherjee B.(Song et al., 2008)	A comprehensive study on backup-bandwidth reprovisioning after network-state updates in survivable telecom mesh networks	2008	IEEE/ACM Transactions on Networking	25	Sun Microsystems, Menlo Park, CA 94025, United States; Department of Computer Science, University of California, Davis, CA 95616, United States	Backup reprovisioning; Mesh; Multiple concurrent failures; Optical; Protection; Restoration; Survivability; Telecom network; WDM	Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
43	Bellavista P., Küpper A., Helal S.(Bellavista et al., 2008)	Location-based services: Back to the future	2008	IEEE Pervasive Computing	136	University of Bologna; Mobile and Distributed Systems Group, Ludwig Maximilian University Munich; Computer and Information Science and Engineering Department, University of Florida	Location-based services; Positioning systems	Article
44	Kwasinski A., Krein P.T.(Kwasinski and Krein, 2007)	Telecom power planning for natural and man-made disasters	2007	INTELEC, International Telecommunications Energy Conference (Proceedings)	10	Grainger Center for Electric Machinery and Electromechanics, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 1406 W. Green Street, Urbana, IL 61801, United States		Conference Paper
45	Hung S.-Y., Yen D.C., Wang H.-Y.(Hung et al., 2006)	Applying data mining to telecom churn management	2006	Expert Systems with Applications	166	Department of Information Management, National Chung Cheng University, Chia-Yi, 62117, Taiwan; Department of DSC, MIS, Miami University, 309 Upham, Oxford, OH 45056, United States; Department of Information Management, National Chung Cheng University, Chia-Yi, 62117, Taiwan	Churn management; Data mining; Decision tree; Neural network; Wireless telecommunication	Article
46	Das, TK and Mohapatro, Arati and Abburu, Sunitha(Das et al., 2015)	A decision making mechanism during disaster event monitoring and control	2015	Middle-East Journal of Scientific Research	1	School of Information Technology & Engineering, VIT University, Vellore, India 1 Department of Computer Science, Bangalore City College, Bangalore, India 2 Department of Computer Applications, Adhiyamaan College of Engineering, Hosur, India	Intuitionistic Fuzzy Set; Rough Set; Public Sentiment; Sentiment Severity	Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
47	Ellinas, Georgios and Stern, Thomas E(Ellinas and Stern, 2001)	Network switch failure restoration	2001	US Patent 6,331,905	40	Columbia University		Patent
48	Wojtasik A., Skoglund B.-E. (Wojtasik and Skoglund, 2003)	Technical risk and economic factors in telecom on-board power design	2003	Conference Proceedings - IEEE Applied Power Electronics Conference and Exposition - APEC	1	Ericsson Power Modules, Manskarsvagen 9, 141 75 Kungens Kurva (Stockholm), Sweden		Conference Paper
49	Salmon, Paul M and Goode, Natassia and Archer, Frank and Spencer, Caroline and McArdle, Dudley and McClure, Roderick J(Salmon et al., 2014)	A systems approach to examining disaster response: using Accimap to describe the factors influencing bushfire response	2014	Safety science	12	University of the Sunshine Coast Accident Research (USCAR), School of Social Sciences, Maroochydore, QLD 4558, Australia;Human Factors Group, Monash Injury Research Institute, Monash University, Building 70, Clayton Campus, Victoria 3800, Australia;	Disaster response; Accimap;System Approach; Human Factor	Article
50	Roos, Inger(Roos, 2002)	Methods of Investigating Critical Incidents A Comparative Review	2002	Journal of Service Research	168	Academy of Finland		Article
51	Sharma, Sachin and Staessens, Dimitri and Colle, Didier and Pickavet, Mario and Demeester, Piet(Sharma et al., 2011)	Enabling fast failure recovery in OpenFlow networks	2011	Design of Reliable Communication Networks (DRCN), 2011 8th International Workshop on the	62	Ghent University - IBBT, Department of Information Technology (INTEC), Gaston Crommenlaan 8, bus 201, 9050 Ghent, Belgium	Carrier Grade Networks;OpenFlow;Protection;Restoration	Conference Paper
52	Shiina, Kazuhito(Shiina, 2013)	A comparative analysis of near-miss falling & slipping incidents at indoor and outdoor telecommunication construction sites	2013	International Conference on Fall Prevention and Protection	2	Sumitomo Densetsu CO. Ltd, Japan		Conference Paper
53	Snow, Andrew P(Snow, 1998)	A Reliability Analysis of Local Telecommunication Switches	1998	Atlanta	1	Department of Computer Information Systems Georgia State University	telecommunication, reliability, switches, public telephone network, ARMIS	TechnicalReport

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
54	Snow, Andrew P and Thayer, M Whiting(Snow and Thayer, 2000)	Defeating telecommunication system fault-tolerant designs	2000	Proceedings of the Third Information Survivability Workshop	9	Department of Computer Information Systems, Georgia State University; Federal Communications Commission, Accounting Safeguards Division		Conference Paper
55	Takács, Márta(Takács, 2010)	Multilevel fuzzy approach to the risk and disaster management	2010	Acta Polytechnica Hungarica	48	John von Neumann Faculty of Informatics, Óbuda University Bécsi út 96/b, H-1034 Budapest, Hungary	risk management; fuzzy multilevel decision making; comparison matrix	Article
56	Tanovic, Anel and Orucevic, Fahrudin and Butkovic, Asmir (Tanovic et al., 2014)	Advantages of the implementation of Service Desk based on ITIL framework in telecommunication industry	2014	2nd International Conference on Wireless and Mobile Communications Systems (WMCS14), Lisbon	1	Department of Computer Science and Informatics University of Sarajevo, Faculty of Electrical Engineering Zmaja od Bosne bb, Sarajevo 71000, Bosnia and Herzegovina	- ITIL, Service Desk, Service Level Management, Supplier Management, Change Management, Event Management, Incident Management, Request Fulfillment, Problem Management	Conference Paper
57	Taylor, William and Massengill, David and Hollingsworth, John(Taylor et al., 2012)	Method and system for automatically identifying a logical circuit failure in a data network	2012	US Patent 8,203,933	19	At&T Intellectual Property I, L.P.		Patent
58	Underwood, Peter and Waterson, Patrick(Underwood and Waterson, 2013)	Systemic accident analysis: examining the gap between research and practice	2013	Accident Analysis & Prevention	42	Loughborough Design School, Loughborough University, Loughborough, Leicestershire, LE11 3TU, UK	Accident analysis; Systems approach; Research-practice gap; STAMP;FRAM; Accimap	Article
59	Wen-Chuan, Yang and Ning-Jun, Chen and Xiao-Yan, Duan (Wen-Chuan et al., 2012)	Research of an Atypical Unexpected Incident in Telecom Complaint Text for 3G	2012	Selected and Revised Results of the 2011 International Conference on Mechanical Engineering and Technology, London, UK	0	Beijing University of Posts and Telecommunication, Beijing, 100876, China	Complaint;Atypical Unexpected Incident; Association rules; Data Mining	Conference

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
60	Otunniyi, IO and Oloruntoba, DT and Seidu, SO (Otunniyi et al., 2018)	Metallurgical analysis of the collapse of a telecommunication tower: Service life versus capital costs tradeoffs	2018	Engineering Failure Analysis	0	Vaal University of Technology, South Africa, The Federal University of Technology Akure, P.M.B. 704, Akure, Nigeria	Communication tower, Material selection, Service life, Cost	Article
61	Frommholz, Ingo and Al-Khateeb, Haider M and Potthast, Martin and Ghasem, Zinnar and Shukla, Mitul and Short, Emma (Frommholz et al., 2016)	On textual analysis and machine learning for cyberstalking detection	2016	Datenbank-Spektrum	6	University of Bedfordshire, Luton, UK, Bauhaus-Universität Weimar, Weimar, Germany"	Cyber security · Cyberstalking · Cyber harassment · Text analytics · Machine learning · Author identification	Articler
62	Choi, Yangseo and Lee, Joo-Young and Choi, Sunoh and Kim, Jong-Hyun and Kim, Ikkyun (Choi et al., 2016)	Introduction to a network forensics system for telecoms analysis	2016	18th International Conference on Advanced Communication Technology (ICACT)	2	Cyber Security Research Division, ETRI, Daejeon, South Korea	Network forensics, cyber blackbox, attack analysis	Conference Paper
63	Lavrova, Daria S (Lavrova, 2016)	An approach to developing the SIEM system for the Internet of Things	2016	Automatic Control and Computer Sciences	7	University of St.Petersburg, Russia	Internet of Things, security incident, data analysis, aggregation, big data arrays, paired relations, self-similarity	Article
64	Gai, Keke and Qiu, Meikang and Elnagdy, Sam Adam (Gai et al., 2016)	A novel secure big data telecom analytics framework for cloud-based cybersecurity insurance	2016	IEEE 2nd International Conference on High Performance and Smart Computing	17	Pace University, New York, NY, 10038, USA	Cybersecurity insurance, incident analytics framework, cloud computing, big data	Conference Paper
65	De Assuncao, Marcos Dias and Cardonha, Carlos Henrique and Koch, Fernando Luiz and Netto, Marco Aurelio Stelmar(De Assuncao et al., 2016)	Facilitating user incident reports	2016	Google Patents	3	International Business Machines Corporation, Armonk, NY, USA	—	Patent
66	Kim, Yang Rae and Park, Myoung Hwan and Jeong, Byung Yong(Kim et al., 2016)	Hazardous Factors and Accident Severity of Cabling Work in Telecommunications Industry	2016	Journal of the Ergonomics Society of Korea	2	Korea	—	Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
67	Fagade, Tesleem and Spyridopoulos, Theo and Albishry, Nabeel and Tryfonas, Theo(Fagade et al., 2017)	System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis	2017	International Conference on Human Aspects of Information Security, Privacy, and Trust	0	Cryptography Group, University of Bristol, Bristol, UK	Malicious insider, Cyber security , Risk modelling , System dynamics , Cyber-risk behaviour , Personality profiling	Conference Paper
68	Bloomfield, Robin E and Popov, Peter and Salako, Kizito and Stankovic, Vladimir and Wright, David (Bloomfield et al., 2017)	Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment	2017	Reliability Engineering & System Safety	1	The Centre for Software Reliability, City, University of London, EC1V 0HB, London, UK b Adelard LLP, 24 Waterside, 44-48 Wharf Road, London N1 7UX, London, UK	Interdependency analysis Risk assessment Cascading failure Critical infrastructure resilienceg	Article
69	Hu, Zhengbing and Gizun, Andrii and Gnatyuk, Viktor and Kotelianets, Vitalii and Zhyrova, Tetiana (Hu et al., 2017)	Method for rules set forming of telecoms extrapolation in network-centric monitoring	2017	4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)	0	Kyiv College of Communication, Kyiv, Ukraine.	cybersecurity; civil aviation; critical aviation information system; identification model; regulatory support; security model; security feature.	Conference Paper
70	Zee, Oscar and Nylander, Tomas and Pelecanos, Dimitrios and Rymert, Lars (Zee et al., 2017)	Method for determining a severity of a network incident	2017	Google Patents	0	Telefonaktiebolaget LM Ericsson (publ), Stockholm (SE)	N/A	Patents
71	Ordóñez, Armando and Eraso, Luis and Ordóñez, Hugo and Merchan, Luis (Ordóñez et al., 2016)	Comparing drools and ontology reasoning approaches for automated monitoring in telecommunication processes	2016	Procedia Computer Science	5	University Foundation of Popayán, 5St 8-58, Popayán, Colombia University of San Buenaventura, Av 10 de Mayo, Cali, Colombia	Service monitoring; automated reconfiguration; ontologies, rules, service composition.	Article
72	Tsakalidis, George and Vergidis, Kostas (Tsakalidis and Vergidis, 2017)	A Systematic Approach Toward Description and Classification of Cybercrime Incidents	2017	IEEE Transactions on Systems, Man, and Cybernetics	1	Department of Applied Informatics, School of Information Sciences, University of Macedonia, Thessaloniki 54 636, Greece	Cybernetics, pattern classification, system analysis and design	Article

Sr. No.	Authors	Title	Year	Source title	Cited by	Affiliations	Keywords	Document Type
73	Hayashi, Koichiro (Hayashi, 2017)	Three Models for Sharing Cybersecurity Incident Information: A Legal and Political Analysis	2017	14th International Telecommunications Society (ITS) Asia-Pacific Regional Conference:	0	Instiotute of Information security, Japan	N/A	Conference Paper
74	Nawawi, Anuar and Salin, Ahmad Saiful Azlin Puteh (Nawawi and Salin, 2018)	Employee fraud and misconduct: empirical evidence from a telecommunication company	2018	Information & Computer Security	0	University of Technology, Malaysia	N/A	Conference Paper

Table 4: Data Extraction for Research Question 1

B Data Extraction from Literature for Research Question 2 & 3

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Dependency	Practice /Research	Pre/post Incident	Comments
1	Probing Human Error as Causal Factor in Incidents with Major Accident Potential (Aas, 2009)	aas2009probing	This paper demonstrates how the Human Factors Assessment and Classification System (HFACS) can be applied to analyze incidents with major accident potential	N/A	N/A	HFACS	No	Practice	Pre (risk)	critical infrastructure
2	Critical Infrastructure Protection in the Information Age (Anderson, 2002)	anderson2002critical	Critical infrastructures consist of physical and information-based facilities, networks and assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security or well being of citizens or on the effective functioning of governments and industries.	System failure	Network failure	NA	No	Practice	Pre (risk)	critical infrastructure
3	Location-based services: Back to the future (Bellavista et al., 2008)	bellavista2008location	It is about 'What Was Wrong with First-Generation Location-Based Services?' an analysis of the incidents happend.	System failure	Mobile services failure	NA	No	Practice	Post	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
4	A multi-agent based decision mechanism for incident reaction in telecommunication network (Bonhomme et al., 2010)	bonhomme2010multi	A global architectural and decision support solution for telecommunication infrastructure from information systems security prespective.	System failure	Network failure	Multi-Agent System reaction architecture	Yes	Practice	Pre (risk)	
5	Mobile System of Recording Incidents in Telecommunications Services: eSUPERTEL (Carrillo and Chamorro, 2014)	carrillo2014mobile	E-government tries to improve the quality of government services especially the telecom facility users	System failure	Mobile network failure	eSUPERTEL	Yes	Practice	post	
6	Examining Human Factors for marine casualties using HFACS-maritime accidents (HFACS-MA) (Chen and Chou, 2012)	chen2012examining	It is about a prototype of the framework for Human Factors Analysis and Classification System for Maritime Accidents (HFACS-MA).	System failure	N/A	Human Factors Analysis and Classification System for Maritime Accidents (HFACS-MA)	No	Practice	Post	
7	A Decision Making Mechanism During Disaster Event Monitoring and Control (Das et al., 2015)	das2015decision	An approach is discussed for handling man made disaster resulting out of propagating sensitive information and rumor..	System failure		N/A	No	Research	Pre (risk)	
8	Organizational accidents investigation methodology and lessons learned (Dien et al., 2004)	dien2004organisational	the understanding of industrial accidents and incidents has evolved, they are no longer considered as the sole product of human and/or technical failures but as originating in an unfavourable organizational context	System failure	-	N/A	No	Research	Post	
9	Combining task analysis and fault tree analysis for accident and incident analysis a case study from Bulgaria (Doytchev and Szwillus, 2009)	doytchev2009combining	Task Analysis in combination with other methods can be applied successfully to human error analysis, revealing details about erroneous actions in a realistic situation.	Human errors	Human error identification	Fault Tree Analysis (FTA) and Task Analysis (TA)	Yes	Research, (Case study)	Post	Hydro power plant,

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Dependency	Practice /Research	Pre/post Incident	Comments
10	Component testing is not enough: A Study of Software Faults in Telecom Middle-ware (Eldh et al., 2007)	eldh2007component	Telecommunication switch outage statistics are analyzed for a multi year period, allowing examination into switch failure frequency, causes, and trends.	System failure	switch failure	time-series-event analysis	Yes	Practice	Post	Analysis is based in other root causes as well
11	Network switch failure restoration (Ellinas and Stern, 2001)	ellinas2001network	invention relates to automatic protection switching systems and methods in networks for restoring switch failures	System failure	Switch failure	N/A	No	Practice	Pre	Patent
12	Topological analysis of cloud service connectivity (Fabian et al., 2015)	fabian2015topological	a study on cloud outages and causes, and analyses the topological connectivity of major cloud service providers (CSPs) by graph-based measures	System failure	Network failure	N/A	No	Practice	Post	protocols
13	Environment friendly high quality, high availability Telecom power plant architecture (Fraisse and Buchsbaum, 2002)	fraisse2002environment	Cost effective alternative power plant proposal	System failure	Power failure	N/A	Yes	Research	Pre	
14	Multi-Agents System Service based Platform in Telecommunication Security Incident Reaction (Gâteau et al., 2009)	gateau2009multi	A global architectural solution built on the requirements for a reaction in case of an alert applied to telecom infrastructures security.	System failure	Security system failure	Multi-agents based Architecture,	Yes	Research	Pre	
15	Un-interruptible Power Supply System for Powering of Telecom Equipment (Goldiner et al., 2000)	goldiner2000uninterruptible	describes the proposed improvement in the reliability of UN-interruptible power supply system for powering of telecom equipment on the basis of redundant connection of AC UPS and Electric Generator.	System failure	power failure	N/A	No	Theory	Post	
16	Performance studies of a self healing network protocol in Telecom Canada long haul networks (Grover et al., 1990)	grover1990performance	a study to verify the speed and routing performance of a newly developed Selfhealing Network (SHN) restoration technique.	System failure	Network Failure	N/A	Yes	Research	Post	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Dependency	Practice /Research	Pre/post Incident	Comments
17	Rack Cooling Effectiveness in DataCenters and Telecom Central Offices: The Rack Cooling Index (RCI) (Herrlin et al., 2005)	herrlin2005rack	proposing a methodology and an index for analyzing the rack cooling effectiveness in data canters, Telecom central offices, and other mission critical facilities.	System failure	Power failure	N/A	No	Theory	Post	
18	Characterizing Large-Scale Routing Anomalies A case study of China Telecom (Hiran et al., 2013)	hiran2013characterizing	China Telecom incident as a case study, to understand (1) what can be learned about large-scale routing anomalies using public data sets, and (2) what types of data should be collected to diagnose routing anomalies in the future.	Malicious actions	IP address	N/A	Yes	Research	Post	hijack of approximately 50,000 IP prefixes in April 2010
19	Applying data mining to telecom churn management (Hung et al., 2006)	hung2006applying	churn management is a major focus of mobile operators and main concern is about churner prediction.	N/A	N/A	Data Mining	No	Research	Pre	
20	Community response grids E-government, social networks, and effective emergency management (Jaeger et al., 2007)	jaeger2007community	explores the viability of using mobile communication technologies and the Web, including e-government, to develop response systems that would aid communities before, during, and after a major disaster, providing channels for contacting residents and responders, uploading information, distributing information, coordinating the responses of social networks, and facilitating resident-to-resident assistance	Natural Phenomena	Disaster	Community Response Grid	Yes	Research,	Pre (Risk)	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
21	Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models (Katsakiori et al., 2009)	katsakiori2009towards	the evolution of accident investigation methods over time reveals a gradual shift from searching for a single immediate cause, to the recognition of multiple causes.	System failure	N/A	N/A	No	Research	Pre	Number of evaluation methods have been discussed
22	Telecom Power Planning for Natural and Man-Made Disasters (Kwasinski and Krein, 2007)	kwasinski2007telecom	It is about planning framework to reduce telecommunication network power supply vulnerability during natural and man-made disasters.	System failure	Power failure, disaster	N/A	Yes	Practice	Post	
23	Telecommunications Power Plant Damage Assessment for Hurricane katrina-site Survey and follow-up Results (Kwasinski et al., 2009)	kwasinski2009telecommunications	knowledge of disaster impact on the telecommunications power infrastructure by discussing the effects of Hurricane Katrina based on an on-site survey conducted in October 2005 and on public sources	System failure	Power failure, disaster	Fault tree analysis	Yes	Practice	Post	
24	A New Accident Analysis Method Based on Complex Network and Cascading Failure (Luo et al., 2013)	luo2013new	an accident investigation method to reveal key causation factors that lead to the final accident	System failure	Network failure,	N/A	Yes	Practice	Pre(Risk)	
25	Applying distributed power modules in Telecom systems (Lindman and Thorsell, 1996)	lindman1996applying	Investigated and classified failures observed in a large complex telecommunication industry middle-ware system	System failure	power failure	N/A	Yes	Research	Pre	fault investigations for software test technique
26	Fusing Information from Tickets and Alerts to Improve the Incident Resolution Process (Salah et al., 2018)	salah2018fusing	Main hypothesis is that incorporating tickets information into the alert correlation process will be beneficial to the incident resolution life-cycle in terms of accuracy, timing, and overall incident's description.	System failure	Network failure	Architecture	Yes	Research	Post	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
27	Solving large-scale real-world telecommunication problems using a grid-based genetic algorithm (Luna et al., 2008)	luna2008solving	The problem, known as automatic frequency planning (AFP), is used in a global system for mobile communications (GSM) networks to assign a number of fixed frequencies to a set of GSM transceivers located in the antennae of a cellular phone network	System failure(Mob)	Mobile Network failure	GrEA-Mathematical	Yes	Theory	Pre	
28	Prescription for disaster: failure to balance structured and unstructured thinking (Mockler, 2003)	mockler2003prescription	Failure to do Manage disaster has led recently to many burst financial bubbles, such as those in the fibre optics, 3G mobile and related telecommunications, computing and technology, and dotcoms.	Natural Phenomena	Disaster	N/A	No	Theory	Post	
29	Rapidly Recovering from the Catastrophic Loss of a Major Telecommunications Office(Morrison, 2011)	morrison2011rapidly	AT & T has a mature network emergency management and business continuity program that plans for and responds to events that affect the AT& T network and its support systems around the globe	System failure	Disaster, Power failure	Incident Management System (IMS)	Yes	Practice	Post	
30	Factors impacting the acceptance of mobile data services–A systematic literature review(Ovčjak et al., 2015)	ovvcjak2015factors	It is about mobile data services and factors that influence their adoption. It is a systematic literature review.	System failure	Mobile network failure	N/A	No	Practice	Post	
31	Rule-based Monitoring and Error Detecting for Converged Telecommunication Processes(Ordóñez et al., 2015)	ordonez2015rule	It is about the management of convergent process in Telecommunication domains where if service fail reconfiguration process recover normal behaviour of composite process.	System failure	Service failure	N/A	No	Practice	Pre	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
32	Disaster monitoring and mitigation using aerospace technologies and integrated telecommunication networks (Pace and Aloi, 2008)	pace2008disaster	Can the use of space technologies and new integrated telecommunication networks mitigate the impact of natural and man made disasters	Natural Phenomena	Disaster	N/A	Yes	Research	Pre (Risk)	Theoretical based on policies making
33	Solving incidents in telecommunications using a multi-agent system (Paolino et al., 2011)	paolino2011solving	This article presents the model and implementation of a multi-agent fuzzy system (MAFS), to automate the search of solutions of incidents in telecommunications,	System failure	Network failure ,	MASF MODEL	yes	Practice	Post	
34	Disaster management and mitigation the telecommunications infrastructure (Patricelli et al., 2009)	patricelli2009disaster	The objective is to design new, potentially attractive telecommunication architectures to better manage a disaster scenario.	Natural Phenomena	Disaster	NGN layered Architecture, MOBSAT	Yes	Theory	Pre (Risk)	
35	Methods of Investigating Critical Incidents A Comparative Review (Roos, 2002)	roos2002methods	Critical incidents have properties that enable valuable information about relationships between service providers and their customers to be stored.	N/A	N/A	Incident analysis based on techniques SPAT, Olsen	Yes	Theory	Pre (Risk)	
36	A systems approach to examining disaster response: Using Accimap to describe the factors influencing bushfire response (Salmon et al., 2014)	salmon2014systems	Risk based human factors methods for examining and enhancing systems of disaster response.	Natural Phenomena	Disaster	Accimap	No	Theory	Pre (Risk)	
37	SafeMesh A wireless mesh network routing protocol for incident area communications (Pirzada et al., 2009)	pirzada2009safemesh	the routing protocol presented, addresses the limitations of current mesh and ad-hoc routing protocols in the context of hybrid WMNs	System failure(Mob)	Mobile Network failure	N/A	Yes	Theory	Post	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
38	Telecom Power Supplies And Power Quality (Redl and Kislovski, 1995)	redl1995telecom	a general discussion of power quality and related global trends,a brief overview of the methods used to achieve compliance with the harmonic regulations.	System failure	Power failure	N/A	Yes	Practice	Post	
39	System and method of diagnosis of incidents and technical support regarding communication services (Salgado et al., 2013)	salgado2013system	System and method of diagnosis of incidents and provision of technical support in a communication service which gathers information both from the user and from previous incidents whose information is stored in a database	System failure	Network Failure	N/A	Yes	Practice	Pre	Patent
40	Disaster-preparedness and recovery a priority for Telecom regulatory authorities (Samarajiva, 2001)	samarajiva2001disaster	theory and practice of regulatory intervention in disaster-preparedness and recovery drawing from a pilot study conducted by the Telecom Regulatory Commission of Sri-Lanka	System failure	Power failure	N/A	Yes	Research	Pre (Risk)	Theoretical based on policies making
41	Enabling fast failure recovery in OpenFlow networks (Sharma et al., 2011)	sharma2011enabling	The goal is to provide a standardized open management interface to the forwarding hardware of a router or switch.	System failure	Network failure	N/A	No	Research	Pre (Risk)	
42	Research on Telecommunication Switching System Survivability Based on Stochastic Petri Net (Shi et al., 2008)	shi2008research	the paper discusses Stochastic Petri Net (SPN) to analyze the survivability characteristics of the telecommunication switching system.	System failure	switch failure	N/A	No	Research	Pre (Risk)	Theoretical based
43	A comparative analysis of near-miss falling & slipping incidents at indoor and outdoor telecommunication construction sites (Shiina, 2013)	shiina2013comparative	It is about clarifying the near-miss falling incidents of telecommunication construction sites.	N/A	N/A	N/A	No	Research	Post	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Dependency	Practice /Research	Pre/post Incident	Comments
44	A Reliability Analysis of Local Telecommunication Switches (Snow, 1998)	snow1998reliability	a reliability analysis of Local Exchange Carrier telecommunication switches in the United States, this study is based on switch outage statistics consisting of switch failure frequency, causes, and trends.	System failure	Switch failure	N/A	No	Research	Post	Find a trend in switch failure over time
45	Defeating Telecommunication System Fault-Tolerant Designs (Snow and Thayer, 2000)	snow2000defeating	Telecommunications carriers sometimes suffer large-scale outages because of the improper deployment or operation of otherwise fault tolerant designs	System failure	Faulty design	N/A	No	Practice	Post	Analyze the causes of outage
46	A comprehensive study on backup-bandwidth re-provisioning after network-state updates in survivable telecom mesh networks (Song et al., 2008)	song2008comprehensive	research works to focus on applying backup-resource re-provisioning when a network failure occurs, for some particular intervals over a certain time period.	System failure	multiple concurrent network failures,	N/A	Yes	Research	Pre	
47	Data from telecommunication networks for incident management (Steenbruggen et al., 2013)	steenbruggen2013data	Use of KPN mobile data for managing traffic incident	System failure(Mob)	Mobile Network failure	N/A	Yes	Research	Post	
48	Power-aware localized routing in wireless networks (Stojmenovic and Lin, 2001)	stojmenovic2001power	We prove that the proposed localized (where each node makes routing decisions based solely on the location of itself, its neighbours, and destination) power, cost, and power-cost efficient routing algorithms are loop-free and show their efficiency by experiments	System failure	Power failure	Algorithm (Mathematical)	No	Theory	Pre	
49	Multilevel fuzzy approach to the risk and disaster management (Takács, 2010)	takacs2010multilevel	A risk management applications is given, with a multilevel risk management method for fuzzy decision making environment	System failure	N/A	N/A	No	Theory	Pre	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
50	Advantages of the im-plementation of Service Desk based on ITIL framework in telecom-munication industry (Tanovic et al., 2014)	tanovic2014advantages	The aim of the paper is to compare the results of normal working a Service Desk before the imple-mentation of ITIL and af-ter the implementation of ITIL.	N/A	Network Failur	N/A	Yes	Practice	Post	
51	Method and system for automatically identifying a logical circuit failure in a data network (Taylor et al., 2012)	taylor2012method	A network management module periodically re-quests trap data indicat-ing the status of the logi-cal connections in the log-ical circuit. After the trap data has been re-ceived by the network management module, the trap data is analysed to determine whether any of the logical connections has failed.	system failure	Network Failure	N/A	No	Practice	Pre	Patent
52	Telecommunication infrastructure in disas-ter:Preparing Cities for Crisis Communication (Townsend and Moss, 2005)	townsend2005telecommunicationsis	partial or complete, the failure of telecommunica-tions infrastructure leads to preventable loss of life and damage to property, by causing delays and errors in emergency re-sponse and disaster relief efforts	Natural Phe-nom-ena	Disaster	N/A	Yes	Theory	Pre(Risk)	Step by step recovery procedure
53	Systemic accident anal-ysis: Examining the gap between research and practice (Underwood and Waterson, 2013)	underwood2013systemic	This research explore the issues stemming from re-search and practice which could hinder the aware-ness, adoption and us-age of Systematic Acci-dent Analysis.	N/A	N/A	Systematic Accident Analysis	No	Theory	Post	Survey

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
54	The state and the threat of cascading failure across critical infrastructure; The implications of empirical evidence from media incident reports (Van Eeten et al., 2011)	van2011state	Cascading failure is seen as potentially catastrophic, extremely difficult to predict and increasingly likely to happen. we find a small number of focused, unidirectional pathways around two infrastructures: energy and telecommunications.	System failure	power failure , Network Failure	N/A	No	Practice	Post	Survey paper
55	Research of an Atypical Unexpected Incident in Telecom Complaint Text for 3G (Wen-Chuan et al., 2012)	wen2012research	About the atypical unexpected small incident which is hard to understand and un-obvious by ordinary.	partial System failure	Network Failure	Metamathematical model and algorithm	No	Practice	Pre	Survey paper
56	Method for remote power fail detection and maintaining continuous operation for data and voice devices operating over local loops (Williams and Lundquist, 1993)	williams1993method	a method and system for identifying and maintaining voice communication in an ISDN type modem system during power fail conditions.	System failure	Network Failure	N/A	No	Practice	Pre	Patent
57	Technical Risk and Economic Factors in Telecom On-board Power Design (Wojtasik and Skoglund, 2003)	wojtasik2003technical	the cost and risk factors involved in the selection of on-board power solutions in Telecom systems.	System failure	Power failure	Distributed Power Architecture	No	Practice	Pre (risk)	
58	Method for detecting security error in mobile telecommunications system and device of telecommunications (Yi et al., 2012)	yi2012method	a method and device for detecting a security error in a security algorithm in use for a PDCP layer of an LTE (Long Term Evolution) system	System failure(Mob)	Mobile Network failure	N/A	No	Practice	Pre	Patent
59	A Recommender System Architecture for Predictive Telecom Network Management (Zaman et al., 2015)	zaman2015recommender	Design and specification of E-Stream, a predictive recommendation based solution to automated network management.	System failure	Switch failure	E-stream	Yes	Research	Pre(risk)	Information based for automation
60	Metallurgical analysis of the collapse of a telecommunication tower: Service life versus capital costs tradeoffs (Otunniyi et al., 2018)	nawawi2018employee	Compliance checking of policies	System Failure	Policy/Procedure flaws	N/A	No	Practice	Post	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Dependency	Practice /Research	Pre/post Incident	Comments
61	On Textual Analysis and Machine Learning for Cyberstalking Detection (Frommholz et al., 2016)	frommholz2016textual	A framework is presented for the detection of text-based cyberstalking and the role and challenges of some core techniques such as author identification, text classification and personalisation	System failure	Cyber security incident	PEN	Yes	Research	Pre(risk)	Cyber security
62	Introduction to a Network Forensics System for Cyber Incidents Analysis (Choi et al., 2016)	choi2016introduction	Suggest a network forensics system, Cyber Black-box,which is focused on the traffic analysis.	System failure	Cyber security incident	Network forensics system	Yes	Research	Post	Cyber security
63	An approach to developing the SIEM system for the Internet of Things (Lavrova, 2016)	lavrova2016approach	Suggests an approach to building systems for analyzing security incidents in the Internet of Things as a self-similar system within the ambit of the normal operation of its constituent objects	System failure	Cyber security incident	N/A	Yes	Research	Post	Cyber security
64	A novel secure big data telecom analytics framework for cloud-based cybersecurity insurance (Gai et al., 2016)	gai2016novel	Proposes a secure cyber incident analytics framework using big data.	System failure	Cyber security incident	Cost-Aware Hierarchical Cyber Incident Analytics (CA-HCIA) Framework	Yes	Research	Pre	Cyber security
65	Facilitating user incident reports (De Assuncao et al., 2016)	de2016facilitating	Discusses incident reporting challenges and give recommendations	N/A	N/A	N/A	No	Practice/Research	Post	
66	Hazardous Factors and Accident Severity of Cabling Work in Telecommunications Industry (Kim et al., 2016)	kim2016hazardous	Draw the characteristics of occupational accidents occurred in cabling work, and assess accident severity based on occupational injury data.	N/A	N/A	N/A	No	Practice	Post	
67	System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis(Fagade et al., 2017)	fagade2017system	Enforcing cybersecurity controls against malicious insiders touches upon complex issues like people, process and technology	System Failure	Cyber attack	System Dynamic approach	Yes	Research	Pre	

Sr.	Name	Key	Description	Initial Root-cause	Subsequent Cause	Method	Domain Depen-dency	Practice /Re-search	Pre/post Inci-dent	Comments
68	Preliminary interde-pendency analysis: An approach to support critical-infrastructure risk-assessment (Bloom-field et al., 2017)	bloomfield2017preliminary	Paper presented a methodology, Prelimi-nary Interdependency Analysis (PIA), for analysing interdepen-dencies between critical infrastructure	N/A	N/A	Interdependency Analysis	Yes	Research	Pre	
69	Method for rules set forming of cyber inci-dents extrapolation in network-centric monitor-ing (Hu et al., 2017)	hu2017method	This work developed a method for rule set form-ing of cyber incident ex-trapolation in Network-centric monitoring.	System Failure	Cyber inci-dent	Rule based telecom Monitoring	Yes	Research	Pre	Metamathematical based
70	Method for determining a severity of a network inci-dent (Zee et al., 2017)	zee2017method	It relates to a method for determining a severity of a network incident caus-ing a network alarm in a communication network..	System Failure	Network Failure	N/A	Yes	Practice	Post	
71	Comparing drools and ontology reasoning ap-proaches for automated monitoring in telecom-munication processes (Ordóñez et al., 2016)	ordonez2016comparing	This article describes the main components of the architecture for monitor-ing module in AUTO framework.	N/A	N/A	AUTO framework	Yes	Research	Pre and Post	
72	A Systematic Approach Toward Description and Classification of Cyber-crime Incidents (Tsaka-lidis and Vergidis, 2017)	tsakalidis2017systematic	Proposes a combinato-rial incident description schema.	N/A	N/A	Incident description Schema	Yes	Research	Pre and Post	
73	Three Models for Shar-ing Cybersecurity Inci-dent Information: A Le-gal and Political Analysis (Hayashi, 2017)	hayashi2017three	Sharing information about cyber security incidents	System Failure	Cyber inci-dent	N/A	Yes	Research	Post	Comparing UK, USA and EU model of information sharing
74	Employee fraud and misconduct: empirical evidence from a tele-communication company (Nawawi and Salin, 2018)	nawawi2018employee	compliance checking	System Failure	N/A	N/A	No	Research	Post	

Table 5: Data Extraction from Literature for RQ3 & RQ2

C Some Telecom Incident Analysis Methods

C.1 E-stream

E-stream is a predictive recommendation based solution for an automated network management. The architecture is designed to handle large networks. E-stream is based on intelligent techniques to predict network incidents and it relates to the predictive symptoms and the occurrence of a particular network scenario. E-Stream not only analyze the possibility of occurrence of an incident but it also gives the human operator control to adapt the decision accordingly. It decompose the complex network incident into small steps and discard redundant steps hence save the information for prediction. It matches the pattern template and propose the solution. This approach is based on autonomic network management (Chaparadza, 2009) where, ever increasing complexity of network is managed by considering multiple affecting factors such as configuration, accounting, security, and equipment performance. E-stream take one step further from autonomic network management by not only identifying network fault but they also predict situation. E-Stream for predictions and recommendations consider two aspects (a) it supports processing events from heterogeneous sources, (b) it addresses the needs of the telecommunication management network. As a combination system E-stream consists of following independent components as shown in Figure 14,

- Data reducer- to reduce the volume of huge telecom input data.
- Correlator- to extract out irrelevant events and correlate important events
- Pattern matcher- to model and identify patterns.
- Predictor- for future learning
- Recommender- to recommend most appropriate solution from the knowledge base.

This system is initially implemented in experimental settings and than as an assistant with an aim to perform automated tasks in real setting.

C.2 eSUPERTEL

eSUPERTEL system is designed for incident recording as well as for suggestions and complaints.This system provide statistics about health of mobile services in a specific region. It is developed on the basis of SUPERTEL in order to record incidents in telecommunications services. These incidents are being recorded in (SM RIT) an application to populate incident database. This application is available on Internet, especially on Facebook and is accessible through various technological devices such as ios/android, smart phones and tactile stands. The main goal is to collect information about claims, complaints, suggestions and failures in the provision of telecommunications services. The SUPERTEL (Superintendence of Telecommunications), is about maintaining and recording user rights in telecommunications services. SUPERTEL used to receive user service requirements, which are needed to be enter into the institution's databases. It is an on-line customer service channel. At first one need to register and later on they can report an incident e.g we can see the incident map in Figure 15 called service complaint map by the Carrillo et al (Carrillo and Chamorro, 2014). Until early 2013, SUPERTEL is used in Ecuador via different service channels. Currently, eSUPERTEL mobile system is used for recording incidents in telecommunications services (SM-RIT) (Carrillo and Chamorro, 2014).

C.3 Software fault Classifier

Software in a typical Telecom system considered as an entity which may become a base of an incident. Moreover, typical Telecom middle-ware software are focused. In total 362 failures are considered for this classification, standard troubleshooting and debugging of the software is considered for these 362 cases (Hiran et al., 2013). The following classes of fault are identified and discussed in literature and recommended for practical use,

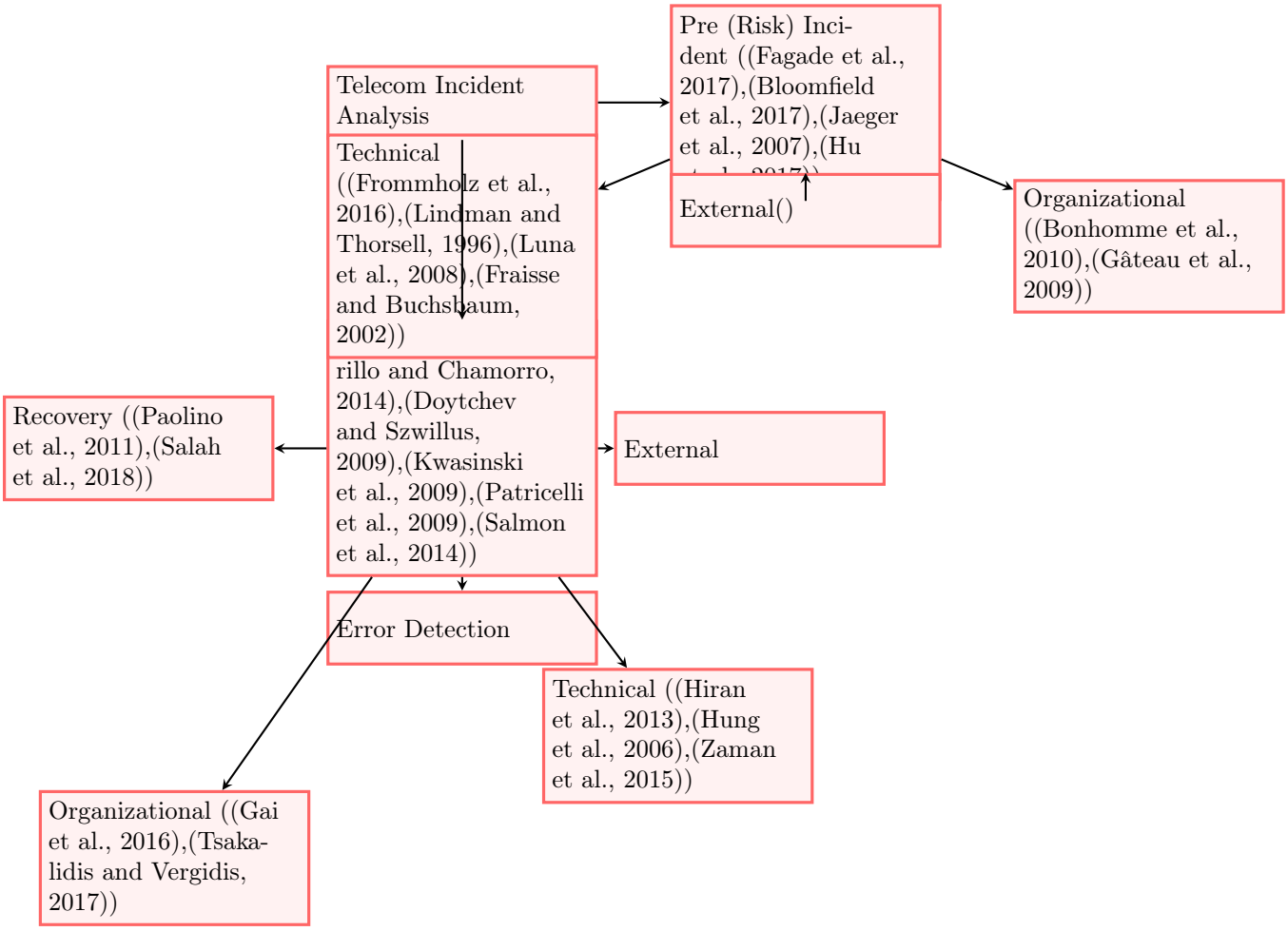

Figure 13: Taxonomy of Incident Analysis

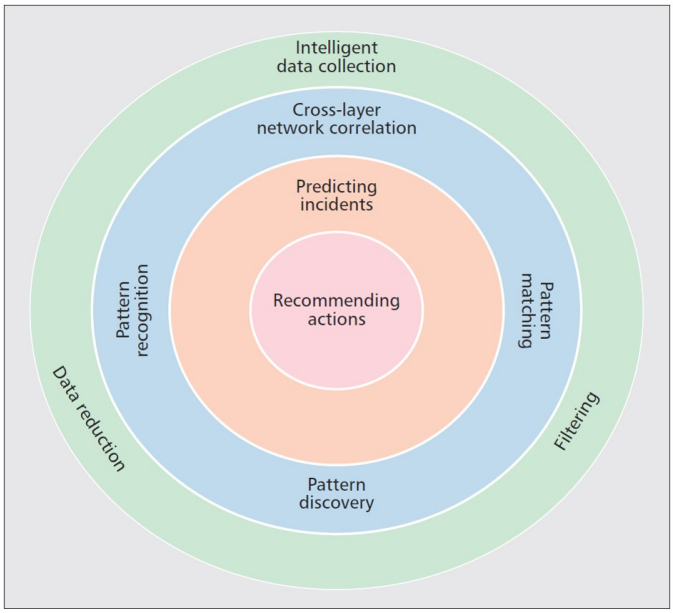

Figure 14: E-Stream Component Layers (Zaman et al., 2015)

Figure 15: Service Complaint Map (Carrillo and Chamorro, 2014)

- Language Pitfalls are faults that are specific to the programming languages.
- Computational/Logical faults are faults inside a computational expression.
- Fault of omission is about missing functionality.
- Spurious faults are also faults of omission, but with too much code where one or several statements need to be removed.
- Function faults, such as calling the wrong function or with wrong parameter.
- Data faults including primitive data faults and composite data fault.
- Resource faults are about memory, stack, and deadlock.
- Third party faults are faults in which we don't have access to the source code.

These fault classifications are foundation to identify the detailed reasons behind an incident cause due to software malfunctioning.

C.4 Multi-agent fuzzy system (MASF)

MASF is designed to find solutions for incidents by using the concepts of multi-agent systems. There exist concept of Subject, Incident, and Severities in MASF model where subject is any component for which an incident may happen. In MASF Incidents are considered as events which effect the subject's normal functioning. Incidents are seen from subjects and events with their severities and available solutions. Incident's severity identify how many subjects are effected by the incident. The MAFS model describes the fuzzy incidents by using six kinds of agents namely GUIUserAgent, GUIAdministratorAgent, SubjectAgent, IncidentAgent, SearchAgent, and DataAcessAgent as seen in Figure 16.

GUIUserAgent and GUIAministratorAgent are interface agents, which are fronted for other agents, humans, and software. SubjectAgent and IncidentAgent are for handling the incidents such as release, modify, eliminate the subject and their incidents. SearchAgent is specialized for search for the incidents' solutions. DataAccessAgents is designed for data manipulation and access. MASF agents can work independently or by the human or another agent (Paolino et al., 2011).

C.5 Situation aware model for telecom

This model is about information content security incidents and telecommunication network themselves,initially a design of situation awareness model was presented. As a whole security situation in the telecommunication network is being analysed and this model is designed based on distributed character data collection and hierarchical progressive integration. Calculation based model can predict incidents as well. Based on structure of model hierarchical information fusion, evidence theory are used to resolve the problem of determining the probability in high level information fusion. Simulation is performed to evaluate the proposed model. Initial simulation results show that the model can compute fast in real time with high accuracy, and can predict incidents effectively after analysis (Lin et al., 2014).

C.6 Switching Path Analysis Technique (SPAT)

The switching path analysis technique (SPAT) is designed to identify the consequences of critical incidents on customers and behavior towards the use of service. SPAT is used as research tool for describing and analyzing customer relationships. It deals with the information stored within critical incidents and policy for customer's sustainability. SPAT not only describes the critical incidents but also it describes criticality of the relationship, switching path leading from the trigger to the telecom relationship switch. Switching path is dependent on 'sustain time' and 'switching time'. According to Roos et al there are multiple triggers involved behind an incident and its switching path (Roos, 2002) as shown in Figure 17. It is concluded that sometimes incidents provide energy to the switching path.

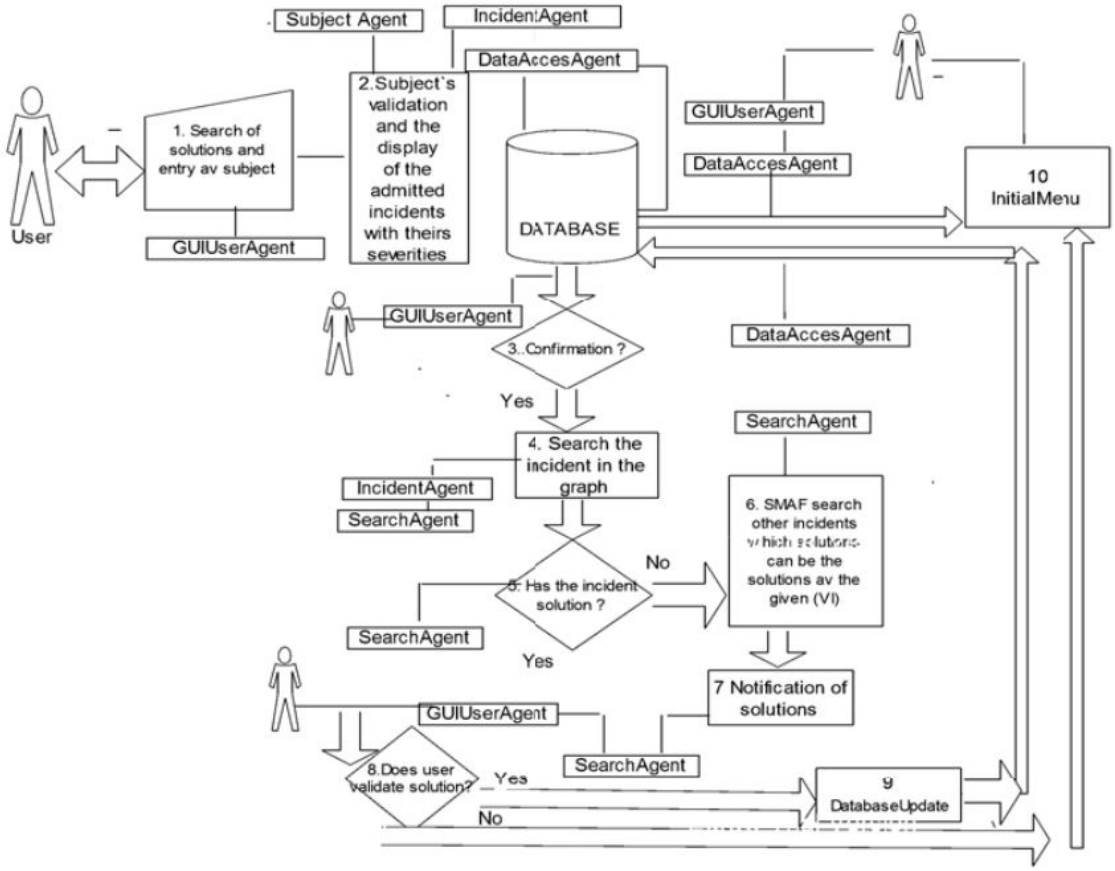

Figure 16: Multi-agent fuzzy system (Paolino et al., 2011)

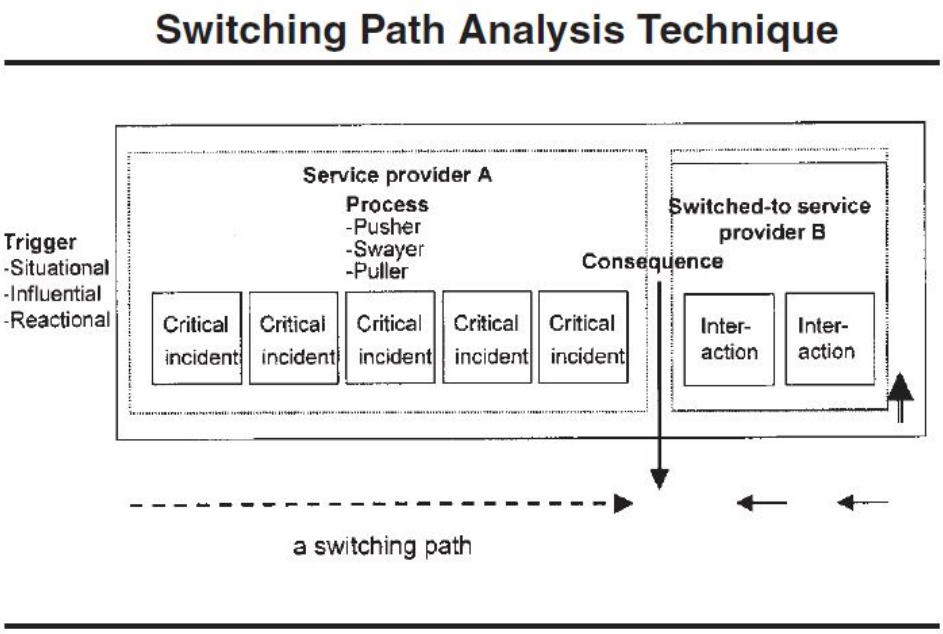

Figure 17: Switching path analysis (Roos, 2002)

D Generalized Incident Analysis Techniques

D.1 Combined Task analysis and fault tree analysis

Fault tree analysis is used to identify the root causes of an accident/incident, while the task analysis is being performed by human and their interaction with environment. To show the validity of the approach, a case study at a Bulgarian Hydro power plant was performed, which shows that task analysis helps to find out which tasks have not/have been performed. In addition to this it shows where the human behavior/reaction to certain situation was the reason of an error. An overview of the types and reasons for incidents have been explored as well.

Figure 18 shows an example of incident where a wireless caller is not being able to place a call. The fault tree for the PSTN is similar. In PSTN cell site controller (CCC) is not needed to administrate calls. Instead in PSTN central offices are interconnected with tandem switches. The cell site controller (CCC) failure is considered separately from the mobile telephony switching offices (MTSOs) failure as cell site controller (CCC) can be located at a different mobile telephony switching offices (MTSOs), which routes the base station calls. Mostly PSTN failure does not cause another PSTN failure. When base stations are replaced by digital loop carriers (DLC), then only a few differences in the distributed infrastructure are. One difference in this branch exists in the DLC isolation cause. Digital loop carriers (DLC) are isolated from its home central office only when the fibre optic link is not damaged. Other difference is non-functioning or failure of antennas or towers. Instead, the corresponding failure cause can be damage in the distribution cables. This failure cause is independent of presence of a Digital loop carrier (DLC). If the Digital loop carrier (DLC) is not there then distribution cable failure is initial event in the distributed element failure. In Figure 18, it is assumed that there is no permanent genset(i.e backup generator) but it has an a/c. Thus the Figure 18 explained the power disruption scenario in detail with the help of fault tree.

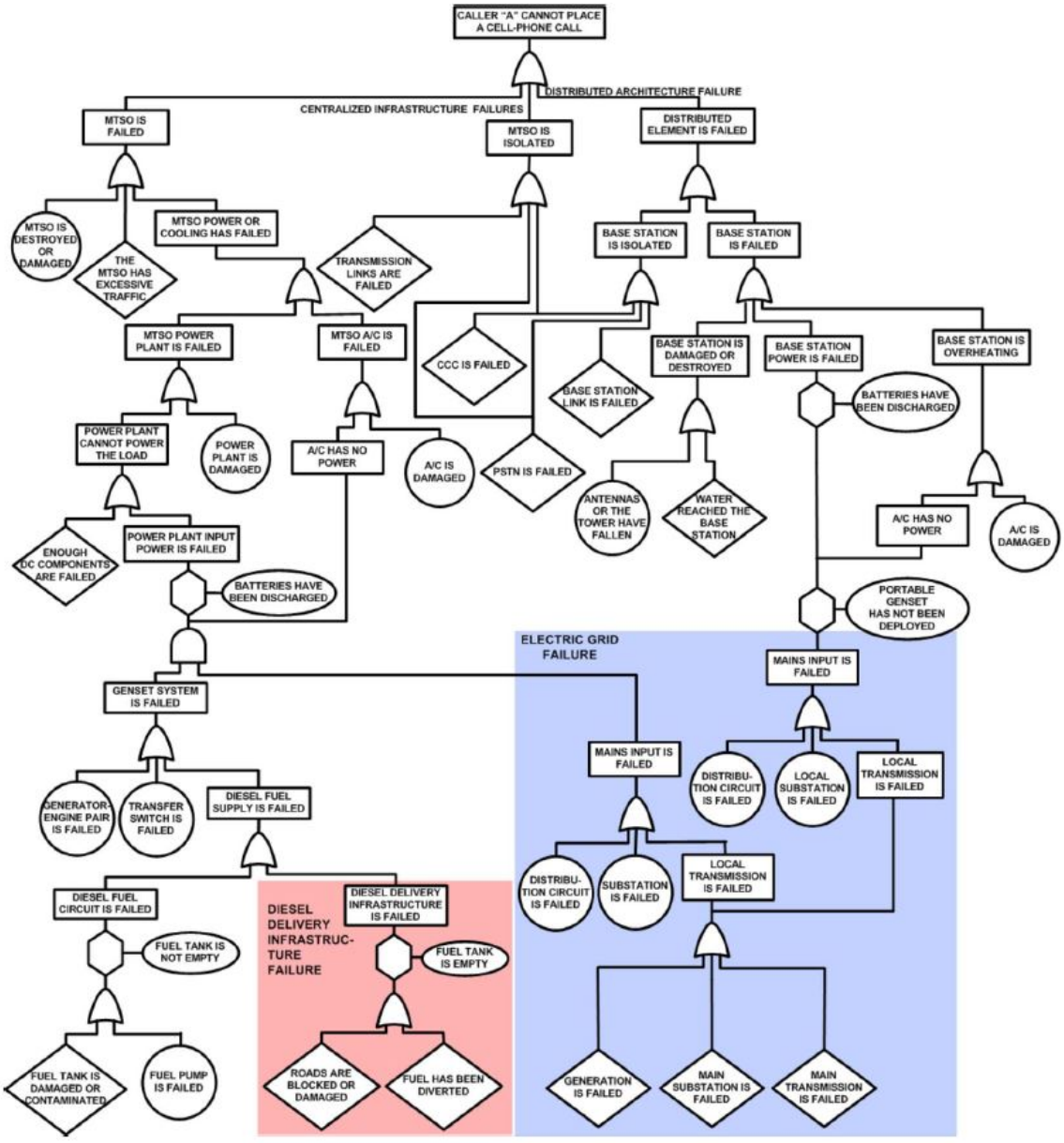

Figure 18: Wireless network fault tree. External power supply branches are highlighted (Kwasinski et al., 2009)

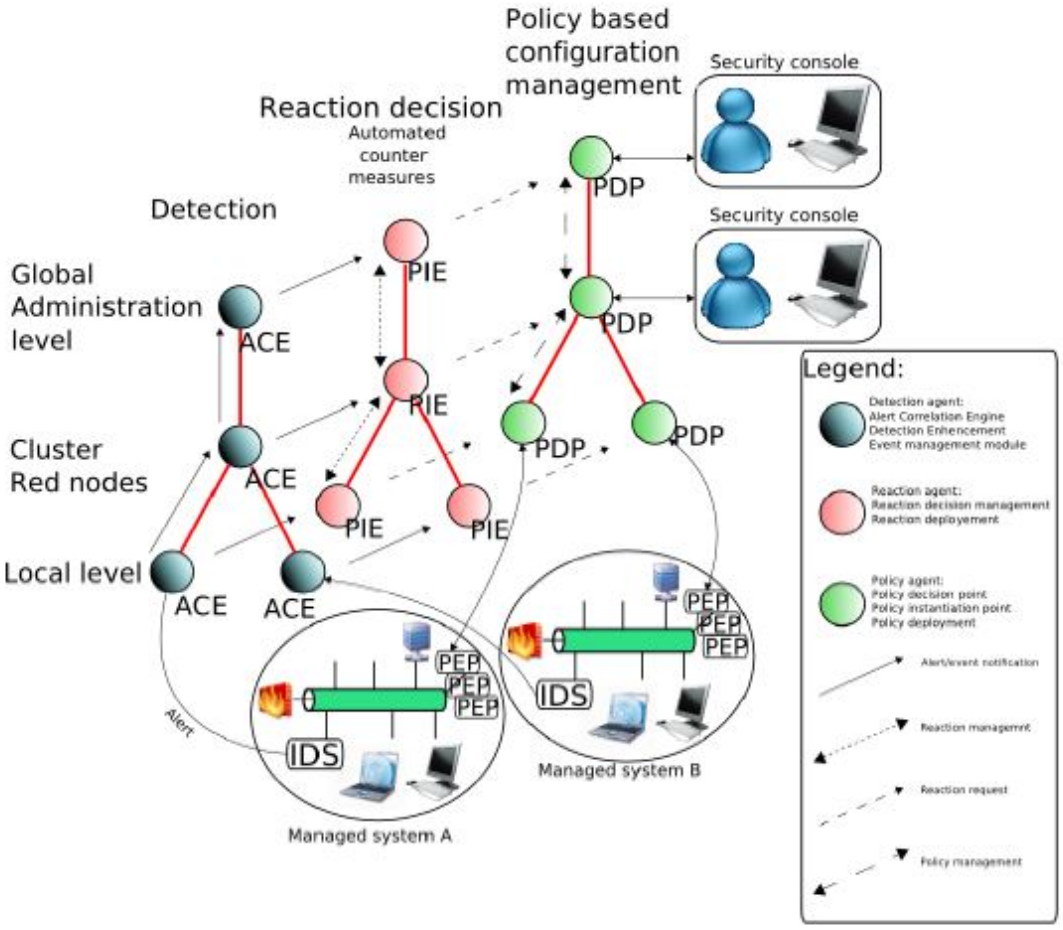

Figure 19: Basic Reaction Architecture (Bonhomme et al., 2010)(Paolino et al., 2011)

D.2 Multi-agent systems

Based on multi-agent system, an architectural and decision support solution for telecom infrastructures has been designed by (Bonhomme et al., 2010) (Paolino et al., 2011) in which incident security and reporting is performed in layered architecture where initial level constitutes the interface between the architecture and the infrastructure, see basic architecture diagram Figure19

Second level correlating the alerts coming from different domains. Agents are used to perform values based decisions. Main ideology, the architecture, which enables the decision making with different levels of knowledge. Another multi agent based architecture to proposed by Gateau (Gâteau et al., 2009) to respond the alert in case some security alert/incident is produced by Telecom infrastructure.

D.3 Human Factors Assessment and Classification System (HFACS)

HFACS is designed to analyze incidents with human impact. Andreas et al discuss the major accident potential and classify the causal factors for the purpose of making a relative comparison of these factors (Aas, 2009). It was explored that at organizational level almost three quarters of all causal factors are due to unsafe human

acts. HFACS is designed to define the latent and active failures in Reason's 'Swiss cheese model' (Shappell and Wiegmann, 2012) with a basis that any system is a production system, which receives input and produces output. An extension in HFACS is HFACS-MA, which is a prototype and in-line with the core concepts of Reason's Generic Error Modelling System (GEMS) and Hawkins's SHEL model (Chen and Chou, 2012) is used for analysis of human factor in maritime accidents. Moreover, it provides a comprehensive insight into the accident regarding disaster. Thus beneficial for spotlighting causalities vulnerability of operations.

D.4 Power Management

Telecommunication is dependent on power system thus reliability of power supply is maintained by distributed ac/dc power modules. Distributed on-board power modules show number of qualities when used in decentralized power systems (Lindman and Thorsell, 1996). Telecommunication requirements such as smaller disablement units, and live insertion is a need for uninterrupted power supply, which is being achieved by the possibility of open interfaces and implementing on-board power modules. Power modules in distributed fashion provide more reliability to the Telecom system but some factors need more consideration such as climatic, environment and equipment mechanics, and similar. Highest efficiency and lowest failure can be achieved if on-board power modules, used in decentralized power systems considered as components. In parallel to distributed power modules Ivan et al (Stojmenovic and Lin, 2001) suggested optimal use of power by power-aware metrics parallel a power-cost metric was also proposed. In case of power disruption we can use the power-aware routing algorithm to minimize the total power needed to route a message between a source and a destination. Power management by using power-cost localized routing algorithm attempts to minimize overall total power needed. Thus, power management can save an incident and also in case it happen distributed power modules help to minimize the risk of Telecom service's un-availability. Power plants architectures are also focused in order to obtain high availability and performance (Fraisse and Buchsbaum, 2002).

D.5 Community response grid (CRG)

Community response grids (CRGs) is the use of Internet and mobile communication devices for communication once an incident happen mostly in disaster situation. It allows people to share information, communicate, and coordinate activities in response to a major disaster. It is the use of mobile communication technologies on the Web for developing response systems before, during, and after a major disaster. Contacting channels can be developed by using this technique for uploading information, distributing information, and facilitating resident-to-resident assistance (Jaeger et al., 2007).Use of social media in combination with telecommunication offer a way in which information can be shared an incident. Sometime incidents are being reported on the social media before they are being identified by the company (Van Eeten et al., 2011). Thus, we can conclude that the social media can play a major role in early identification of incident.

D.6 MOBSAT

Layered architecture: Fundamental requirements of disaster management include the communication of information to and from the disaster area. Many recent disaster management exercises show that rescue efforts are greatly hampered by incidents of the telecommunications systems. MOBSAT is an approach proposed particularly in environments where the usual telecommunication platforms are either disrupted or non-functional due to an incident caused by disaster. Following are the guidelines proposed for temporary reinstate of telecommunication infrastructure in case of emergency,

- Replacement should be simple in use and require minimal field maintenance,
- Replacement must be operated by personnel who are unskilled in advanced telecommunications,
- Replacement must be rugged enough to permit all-weather,
- Replacement should be multimedia capable (data/voice/video) ,

- Replacement should be capable of sustaining heavy, bi-directional, multi-channel traffic (high-bandwidth capability and bandwidth redundancy).

As Compared to proposed solutions of incident management, the architecture proposed by Patricelli (Patricelli et al., 2009) satisfies most of the required criteria. It permits quick restoration of the damaged distribution network to its pre-disaster capacity. Moreover, it is flexible, lighter and cheaper. For example a MOBSAT unit hauled by a common car and eventually a balloon are all that is needed.

References

Aas, A. L. (2009). Probing human error as causal factor in incidents with major accident potential. In *Digital Society, 2009. ICDS'09. Third International Conference on*, pages 272–276. IEEE.

Anderson, P. S. (2002). Critical infrastructure protection in the information age. *Networking Knowledge for Information Societies: Institutions & Intervention*.

Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33.

Bellavista, P., Kupper, A., and Helal, S. (2008). Location-based services: Back to the future. *Pervasive Computing, IEEE*, 7(2):85–89.

Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., and Wright, D. (2017). Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering & System Safety*, 167:198–217.

Bonhomme, C., Feltus, C., and Khadraoui, D. (2010). A multi-agent based decision mechanism for incident reaction in telecommunication network. In *ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010*, pages 1–2. IEEE.

Branford, K., Hopkins, A., Naikar, N., et al. (2009). Guidelines for accimap analysis. In *Learning from high reliability organisations*. CCH Australia Ltd.

Carrillo, B. and Chamorro, S. (2014). Mobile system of recording incidents in telecommunications services: esupertel. In *eDemocracy & eGovernment (ICEDEG), 2014 First International Conference on*, pages 113–118. IEEE.

Chaparadza, R. (2009). Unifaff: a unified framework for implementing autonomic fault management and failure detection for self-managing networks. *International Journal of Network Management*, 19(4):271–290.

Chen, S.-T. and Chou, Y.-H. (2012). Examining human factors for marine casualties using hfacs-maritime accidents (hfacs-ma). In *ITS Telecommunications (ITST), 2012 12th International Conference on*, pages 391–396. IEEE.

Choi, Y., Lee, J.-Y., Choi, S., Kim, J.-H., and Kim, I. (2016). Introduction to a network forensics system for cyber incidents analysis. In *Advanced Communication Technology (ICACT), 2016 18th International Conference on*, pages 50–55. IEEE.

Das, T., Mohapatro, A., and Abburu, S. (2015). A decision making mechanism during disaster event monitoring and control. *Middle-East Journal of Scientific Research*, 23(9):2251–2255.

De Assuncao, M. D., Cardonha, C. H., Koch, F. L., and Netto, M. A. S. (2016). Facilitating user incident reports. US Patent 9,418,354.

Dekker, M., Liveri, D., Catteddu, D., and Dupr, L. (2011). Technical guideline for minimum security measures:guidance on the security measures in article 13a. Technical report.

Dien, Y., Llory, M., and Montmayeul, R. (2004). Organisational accidents investigation methodology and lessons learned. *Journal of Hazardous Materials*, 111(1):147–153.

Doytchev, D. E. and Szwillus, G. (2009). Combining task analysis and fault tree analysis for accident and incident analysis: a case study from bulgaria. *Accident Analysis & Prevention*, 41(6):1172–1179.

Eldh, S., Punnekkat, S., and Hansson, H. (2007). Jönsson., p.: Component testing is not enough-a study of software faults in telecom middleware. In *Proc. 19th IFIP Int Conf. on Testing of Comm. Syst TESTCOM/FATES*.

Ellinas, G. and Stern, T. E. (2001). Network switch failure restoration. US Patent 6,331,905.

European Union Agency For Network And Information Security (2014). Annual incident reports 2013. Annual report.

European Union Agency For Network And Information Security (2015). Annual incident reports 2014. Annual report.

European Union Agency For Network And Information Security (2016). Annual incident reports 2015. Annual report.

European Union Agency For Network And Information Security (2017). Annual incident reports 2016. Annual report.

Fabian, B., Baumann, A., and Lackner, J. (2015). Topological analysis of cloud service connectivity. *Computers & Industrial Engineering*, 88:151–165.

Fagade, T., Spyridopoulos, T., Albishry, N., and Tryfonas, T. (2017). System dynamics approach to malicious insider cyber-threat modelling and analysis. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 309–321. Springer.

Fraisse, M. and Buchsbaum, L. (2002). Environment friendly high quality, high availability telecom power plant architecture. In *Telecommunications Energy Conference, 2002. INTELEC. 24th Annual International*, pages 463–469. IEEE.

Frommholz, I., Al-Khateeb, H. M., Potthast, M., Ghasem, Z., Shukla, M., and Short, E. (2016). On textual analysis and machine learning for cyberstalking detection. *Datenbank-Spektrum*, 16(2):127–135.

Gai, K., Qiu, M., and Elnagdy, S. A. (2016). A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. In *Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on*, pages 171–176. IEEE.

Gâteau, B., Khadraoui, D., and Feltus, C. (2009). Multi-agents system service based platform in telecommunication security incident reaction. In *2009 Global Information Infrastructure Symposium*, pages 1–6. IEEE.

Goldiner, A., Golovko, V., and Ljubelskiy, A. (2000). Uninterruptible power supply system for powering of telecom equipment. In *Telecommunications Energy Special Conference, 2000. TELESCON 2000. The Third International*, pages 251–253. IEEE.

Grover, W., Venables, B., Sandham, J., and Mine, A. (1990). Performance studies of a selfhealing network protocol in telecom canada long haul networks. In *Global Telecommunications Conference, 1990, and Exhibition.'Communications: Connecting the Future', GLOBECOM'90., IEEE*, pages 452–458. IEEE.

Harzing, A.-W. and Alakangas, S. (2016). Google scholar, scopus and the web of science: a longitudinal and cross-disciplinary comparison. *Scientometrics*, 106(2):787–804.

Hayashi, K. (2017). Three models for sharing cybersecurity incident information: A legal and political analysis.

Herrlin, M. K. et al. (2005). Rack cooling effectiveness in data centers and telecom central offices: The rack cooling index (rci). *Transactions-American Society of Heating Refrigerating and Air conditioning Engineers*, 111(2):725.

Hiran, R., Carlsson, N., and Gill, P. (2013). Characterizing large-scale routing anomalies: a case study of the china telecom incident. In *Passive and Active Measurement*, pages 229–238. Springer.

Hu, Z., Gizun, A., Gnatyuk, V., Kotelianets, V., and Zhyrova, T. (2017). Method for rules set forming of cyber incidents extrapolation in network-centric monitoring. In *Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International*, pages 444–448. IEEE.

Hung, S.-Y., Yen, D. C., and Wang, H.-Y. (2006). Applying data mining to telecom churn management. *Expert Systems with Applications*, 31(3):515–524.

ISO (2005). Information technology — service management — part 1: Service management system requirements. ISO standard.

Jaeger, P. T., Shneiderman, B., Fleischmann, K. R., Preece, J., Qu, Y., and Wu, P. F. (2007). Community response grids: E-government, social networks, and effective emergency management. *Telecommunications Policy*, 31(10):592–604.

Katsakiori, P., Sakellaropoulos, G., and Manatakis, E. (2009). Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. *Safety Science*, 47(7):1007–1015.

Kim, Y. R., Park, M. H., and Jeong, B. Y. (2016). Hazardous factors and accident severity of cabling work in telecommunications industry. *Journal of the Ergonomics Society of Korea*, 35(3).

Kitchenham, B. A., Budgen, D., and Brereton, P. (2015). *Evidence-Based Software Engineering and Systematic Reviews*, volume 4. CRC Press.

Kuhrmann, M., Fernández, D. M., and Daneva, M. (2016). On the pragmatic design of literature studies in software engineering: an experience-based guideline. *Empirical Software Engineering*, pages 1–40.

Kwasinski, A. and Krein, P. T. (2007). Telecom power planning for natural and man-made disasters. In *Telecommunications Energy Conference, 2007. INTELEC 2007. 29th International*, pages 216–222. IEEE.

Kwasinski, A., Weaver, W. W., Chapman, P. L., and Krein, P. T. (2009). Telecommunications power plant damage assessment for hurricane katrina–site survey and follow-up results. *Systems Journal, IEEE*, 3(3):277–287.

Lavrova, D. S. (2016). An approach to developing the siem system for the internet of things. *Automatic Control and Computer Sciences*, 50(8):673–681.

Lekberg, A. (1997). Different approaches to incident investigation-how the analyst makes a difference. *Hazard Prevention*, 33:10–15.

Lin, G., Xinsheng, J., and Tao, J. (2014). Research on situation awareness model of information content security incidents in telecommunication network. *Telecommunications Science*, 30(2):14–20.

Lindman, P. and Thorsell, L. (1996). Applying distributed power modules in telecom systems. *Power Electronics, IEEE Transactions on*, 11(2):365–373.

Luna, F., Nebro, A. J., Alba, E., and Durillo, J. J. (2008). Solving large-scale real-world telecommunication problems using a grid-based genetic algorithm. *Engineering Optimization*, 40(11):1067–1084.

Luo, Z., Li, K., Ma, X., and Zhou, J. (2013). A new accident analysis method based on complex network and cascading failure. *Discrete Dynamics in Nature and Society*, 2013.

Mockler, R. J. (2003). Prescription for disaster: failure to balance structured and unstructured thinking. *Business Strategy Review*, 14(2):17–25.

Molloy, G. J. and O'Boyle, C. A. (2005). The shel model: a useful tool for analyzing and teaching the contribution of human factors to medical error. *Academic Medicine*, 80(2):152–155.

Mongeon, P. and Paul-Hus, A. (2016). The journal coverage of web of science and scopus: a comparative analysis. *Scientometrics*, 106(1):213–228.

Morrison, K. T. (2011). Rapidly recovering from the catastrophic loss of a major telecommunications office. *Communications Magazine, IEEE*, 49(1):28–35.

Nawawi, A. and Salin, A. S. A. P. (2018). Employee fraud and misconduct: empirical evidence from a telecommunication company. *Information & Computer Security*, 26(1):129–144.

Ordóñez, A., Eraso, L., and Falcarin, P. (2015). Rule-based monitoring and error detecting for converged telecommunication processes. In *SAI Intelligent Systems Conference (IntelliSys), 2015*, pages 705–713. IEEE.

Ordóñez, A., Eraso, L., Ordóñez, H., and Merchan, L. (2016). Comparing drools and ontology reasoning approaches for automated monitoring in telecommunication processes. *Procedia Computer Science*, 95:353–360.

Otunniyi, I., Oloruntoba, D., and Seidu, S. (2018). Metallurgical analysis of the collapse of a telecommunication tower: Service life versus capital costs tradeoffs. *Engineering Failure Analysis*, 83:125–130.

Ovčjak, B., Heričko, M., and Polančič, G. (2015). Factors impacting the acceptance of mobile data services–a systematic literature review. *Computers in Human Behavior*, 53:24–47.

Pace, P. and Aloi, G. (2008). Disaster monitoring and mitigation using aerospace technologies and integrated telecommunication networks. *Aerospace and Electronic Systems Magazine, IEEE*, 23(4):3–9.

Paolino, L., Paggi, H., Alonso, F., and López, G. (2011). Solving incidents in telecommunications using a multi-agent system. In *Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on*, pages 303–308. IEEE.

Patricelli, F., Beakley, J. E., Carnevale, A., Tarabochia, M., and Von Lubitz, D. K. (2009). Disaster management and mitigation: the telecommunications infrastructure. *Disasters*, 33(1):23–37.

Pirzada, A. A., Portmann, M., Wishart, R., and Indulska, J. (2009). Safemesh: A wireless mesh network routing protocol for incident area communications. *Pervasive and Mobile Computing*, 5(2):201–221.

Redl, R. and Kislovski, A. S. (1995). Telecom power supplies and power quality. In *Telecommunications Energy Conference, 1995. INTELEC'95., 17th International*, pages 13–21. IEEE.

Roos, I. (2002). Methods of investigating critical incidents a comparative review. *Journal of Service Research*, 4(3):193–204.

Salah, S., Maciá-Fernández, G., and Díaz-Verdejo, J. E. (2018). Fusing information from tickets and alerts to improve the incident resolution process. *Information Fusion*.

Salgado, J. A. P., Duran, J. M. M., Poza, J. M. R., and Gallego, M. L. (2013). System and method of diagnosis of incidents and technical support regarding communication services. US Patent App. 13/816,363.

Salmon, P. M., Goode, N., Archer, F., Spencer, C., McArdle, D., and McClure, R. J. (2014). A systems approach to examining disaster response: Using accimap to describe the factors influencing bushfire response. *Safety science*, 70:114–122.

Samarajiva, R. (2001). Disaster-preparedness and recovery: a priority for telecom regulatory agencies in liberalized environments. *International Journal of Regulation and Governance*, 1(2):181–196.

Shappell, S. A. and Wiegmann, D. A. (2012). *A human error approach to aviation accident analysis: The human factors analysis and classification system*. Ashgate Publishing, Ltd.

Sharma, S., Staessens, D., Colle, D., Pickavet, M., and Demeester, P. (2011). Enabling fast failure recovery in openflow networks. In *Design of Reliable Communication Networks (DRCN), 2011 8th International Workshop on the*, pages 164–171. IEEE.

Shi, T., Zhao, J., Yin, X., and Wang, J. (2008). Research on telecommunication switching system survivability based on stochastic petri net. In *Innovative Computing Information and Control, 2008. ICICIC'08. 3rd International Conference on*, pages 413–413. IEEE.

Shiina, K. (2013). A comparative analysis of near-miss falling & slipping incidents at indoor and outdoor telecommunication construction sites. In *International Conference on Fall Prevention and Protection*, pages 211–216.

Snow, A. P. (1998). A reliability analysis of local telecommunication switches. *Atlanta*.

Snow, A. P. and Thayer, M. W. (2000). Defeating telecommunication system fault-tolerant designs. In *Proceedings of the Third Information Survivability Workshop (ISW 2000)*, pages 24–26.

Song, L., Zhang, J., and Mukherjee, B. (2008). A comprehensive study on backup-bandwidth reprovisioning after network-state updates in survivable telecom mesh networks. *IEEE/ACM Transactions on Networking*, 16(6):1366–1377.

Steenbruggen, J., Borzacchiello, M. T., Nijkamp, P., and Scholten, H. (2013). Data from telecommunication networks for incident management: An exploratory review on transport safety and security. *Transport policy*, 28:86–102.

Stojmenovic, I. and Lin, X. (2001). Power-aware localized routing in wireless networks. *Parallel and Distributed Systems, IEEE Transactions on*, 12(11):1122–1133.

Takács, M. (2010). Multilevel fuzzy approach to the risk and disaster management. *Acta Polytechnica Hungarica*, 7(4):91–102.

Tanovic, A., Orucevic, F., and Butkovic, A. (2014). Advantages of the implementation of service desk based on itil framework in telecommunication industry. In *2nd International Conference on Wireless and Mobile Communications Systems (WMCS14), Lisbon*.

Taylor, W., Massengill, D., and Hollingsworth, J. (2012). Method and system for automatically identifying a logical circuit failure in a data network. US Patent 8,203,933.

Townsend, A. and Moss, M. (2005). Telecommunications infrastructure in disasters: Preparing cities for crisis communications: Tech. *Rep. of Robert F. Wagner Graduate School of Public Service, New York University*.

Tsakalidis, G. and Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*.

Underwood, P. and Waterson, P. (2013). Systemic accident analysis: examining the gap between research and practice. *Accident Analysis & Prevention*, 55:154–164.

Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., and Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. *Public Administration*, 89(2):381–400.

Wen-Chuan, Y., Ning-Jun, C., and Xiao-Yan, D. (2012). Research of an atypical unexpected incident in telecom complaint text for 3g. In *Mechanical Engineering and Technology*, pages 647–652. Springer.

Wienen, H. C. A., Bukhsh, F. A., Vriezekolk, E., and Wieringa, R. J. (2017). Accident analysis methods and models—a systematic literature review. *CTIT Technical Report*, (TR-CTIT-17-04).

Williams, A. B. and Lundquist, D. T. (1993). Method for remote power fail detection and maintaining continuous operation for data and voice devices operating over local loops. US Patent 5,216,704.

Wojtasik, A. and Skoglund, B.-E. (2003). Technical risk and economic factors in telecom on-board power design. In *Applied Power Electronics Conference and Exposition, 2003. APEC'03. Eighteenth Annual IEEE*, volume 2, pages 786–789. IEEE.

Yi, S.-J., Park, S.-J., Lee, Y.-d., and Chun, S.-D. (2012). Method for detecting security error in mobile telecommunications system and device of mobile telecommunications. US Patent 8,243,931.

Zaman, F., Hogan, G., Der Meer, S., Keeney, J., Robitzsch, S., and Muntean, G.-M. (2015). A recommender system architecture for predictive telecom network management. *Communications Magazine, IEEE*, 53(1):286–293.

Zee, O., Nylander, T., Pelecanos, D., and Rymert, L. (2017). Method for determining a severity of a network incident. US Patent 9,680,722.