Virtually all functions in modern society depend on information technology (IT) systems and their uninterruptible operation. This thesis aims to explain what the typical root causes of unplanned IT service interruptions, incidents and what their contributing factors are. The IT service incident model (IIModel), other tools and methods are developed in order to understand the underlying conditions to incidents, to prevent their reoccurrence and to improve the IT service quality.
KARI SAARELAINEN

How and why things happen - Anatomy of IT service incidents

Publications of the University of Eastern Finland
Dissertations in Forestry and Natural Sciences
No 238

Academic Dissertation
To be presented by permission of the Faculty of Science and Forestry for public examination in the Auditorium CA102 Canthia Building at the University of Eastern Finland, Kuopio, on November 25, 2016, at 13 o’clock.
Department of Computer Science
Author’s address: Vanhaväylä 39A
00830 HELSINKI, FINLAND
email:kari.saarelainen@iki.fi

Supervisors: Head of Research Marko Jäntti, PhD
University of Eastern Finland
School of Computing
P.O.Box 1627
70211 KUOPIO, FINLAND
email: marko.jantti@uef.fi

University Lecturer Matti Nykänen, PhD
University of Eastern Finland
School of Computing
P.O.Box 1627
70211 KUOPIO, FINLAND
email: matti.nykanen@uef.fi

Reviewers: Professor Aileen Cater-Steel, Ph.D.
University of Southern Queensland
School of Management and Enterprise
Toowoomba Campus
4350 QUEENSLAND, AUSTRALIA
email: Aileen.Cater-Steel@usq.edu.au

Associate Professor Mira Kajko-Mattsson, PhD
KTH Royal Institute of Technology
School of Information and Communication Technology
Electrum 229
10044 STOCKHOLM, SWEDEN
email: mekm2@kth.se

Opponent: Senior Researcher Tomi Dahlberg, PhD
Turku School of Economics at the University of Turku
20014 UNIVERSITY OF TURKU, FINLAND
email: tomi.dahlberg@utu
and
Executive in Residence
Aalto University School of Business
00076 AALTO, FINLAND
email (secondary): tomi.dahlberg@aalto.fi
ABSTRACT:

Virtually all functions in modern society depend on information technology (IT) systems and their reliable operation. Regardless, unplanned IT service breaks and degradation of service quality (i.e. incidents) does occur. IT service incident costs in North America may be as high as 4% of the gross domestic product (GDP).

The primary objective of this thesis was to determine why IT service incidents occur, how they are contributed to by latent or active factors, and how this information could be used to prevent the reoccurrence of the incidents. The IT service incidents were modelled using accident investigations and accident models commonly applied in other industries. The IT incident data consisted of over 200 hundred written incident reports; these were supplemented by interviews, documentation, information from a variety of tools, and an analysis of the aspects related to an organisation, its teamwork and processes.

IT service incidents differ from incidents and accidents in other industries. The existing incident models were therefore not considered suitable to IT service incidents. A hierarchical classification taxonomy was developed to the root causes of IT service incidents and their contributing conditions and factors. Additionally, a simple presentation method was developed to present the events and the causal factors related to the incidents.

The incidents and their causal factors, with the conditional probabilities, were analysed in a Bayesian Belief Network (BBN). The BBN was used to analyse the contributing factors of the incidents and evaluate the effect of changing factors in the organisation. For the incident investigation, a new analytics method was developed to analyse the large numbers of incidents. These four tools and methods were presented in different phases of proactive problem management, which identifies trends or significant problems analysing incident records. These tools can be used by problem managers and quality managers to improve the problem management process and quality of IT services.
Universal Decimal Classification: 004.052, 004.416, 005.332.7, 005.334, 005.336.3

Library of Congress Subject Headings: Information technology; Computer systems; Computer system failures; Software maintenance; Problem solving; Errors; Root cause analysis; Quality assurance

Yleinen suomalainen asiasanasto: tietotekniikka; tietojärjestelmät; häiriöt; toimintahäiriöt; ongelmat; virheet; virhetilanteet; virheanalyysi; sytyt; ylläpito; käyttövarmuus; luotettavuus; ongelmanratkaisu; laadunvarmistus
This work would not have been possible without the help of a large group of people. First of all, I would like to thank my supervisors, Dr. Marko Jäntti and Dr. Matti Nykänen, for their support with the thesis. Additionally, Marko also acting as a co-writer on the publications has been an invaluable guide to this novice researcher taking his first journey into the wilderness of science. Dr. Mika Hujo, with his special expertise, was an essential element in one of the publications.

The practical part of the research was performed in the IT advisory department of KPMG Finland, and in its client engagements. I would like to thank the head of IT advisory, Janne Vesa, and head of management consulting, Harri Wihuri, for allowing me the opportunity to prepare my thesis. An extensive amount of work in analysis of incidents in various engagements has been done. My warm thanks goes to my colleagues, who have worked with the engagements used in this thesis: Heikki Saarinen, Tommi Perasto, Markus Saviaro, Asko Torniainen, Antti-Jussi Kangas, Terhi Lehtonen and Jarmo Törmänen. The undisclosed case organisations and their representatives are acknowledged for interesting projects and for their interest in improvement of IT service quality.

Professor Aileen Cater-Steel and associate professor Mira Kajko-Mattsson certainly deserve acknowledgement for their thorough review of the thesis and publications and for their comments. Thanks to Dr. Tomi Dahlberg, who has devoted time away from other professional and personal activities to review this work and to act as an opponent in defence of this thesis.

I am grateful to my parents, Aini and Erkki Saarelainen, who raised me with the values eventually leading to this thesis. My thanks to Tarja and Jarmo Niemi and Kirsi and Jukka Hammar for their valuable and in-depth comments regarding protocol, dress code and arrangement of social activities after the
dissertation. Hannu Kuitunen also deserves acknowledgement for being the first person to register in the party after the dissertation. Last, but not least, I want to thank my family, my wife Ann-Marie, my daughter Annina and my son Herman, for their patience, support and love. Special thanks to Ann-Marie for her contribution to science in the form of coffee and sandwiches delivered to the research facility.

Helsinki, October 25, 2016       Kari Saarelainen
Felix qui potuit rerum cognoscere causas

Fortunate is he, who is able to understand the causes of things

Virgil (70 - 19 BC): “Georgics” (29 BC)
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAIB</td>
<td>Aircraft Accident Investigation Bureau</td>
</tr>
<tr>
<td>ATSB</td>
<td>Australian Transport Safety Bureau</td>
</tr>
<tr>
<td>BBN</td>
<td>Bayesian Belief Network</td>
</tr>
<tr>
<td>BSI</td>
<td>British Standards Institution</td>
</tr>
<tr>
<td>CI</td>
<td>configuration item</td>
</tr>
<tr>
<td>CMDB</td>
<td>configuration management database</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technology</td>
</tr>
<tr>
<td>CSI</td>
<td>continual service improvement</td>
</tr>
<tr>
<td>ECFC</td>
<td>events and causal factors chart</td>
</tr>
<tr>
<td>ELK</td>
<td>Elastic Search, Logstash, Kibana</td>
</tr>
<tr>
<td>ESReDA</td>
<td>European Safety, Reliability and Data Association</td>
</tr>
<tr>
<td>eTOM</td>
<td>Business Process Framework</td>
</tr>
<tr>
<td>FRAM</td>
<td>Functional Resonance Accident Model</td>
</tr>
<tr>
<td>FTA</td>
<td>fault tree analysis</td>
</tr>
<tr>
<td>GDP</td>
<td>gross domestic product</td>
</tr>
<tr>
<td>HERA</td>
<td>Human Error in European Air Traffic Management</td>
</tr>
<tr>
<td>HFACS</td>
<td>Human Factors Analysis and Classification System</td>
</tr>
<tr>
<td>HTO</td>
<td>Human-Technology-Organisation</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communications technology</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IIModel</td>
<td>IT Incident Model</td>
</tr>
<tr>
<td>ITIL</td>
<td>IT Infrastructure Library</td>
</tr>
<tr>
<td>ISACA</td>
<td>Information Systems Audit and Control Association</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organisation</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>ITSM</td>
<td>IT service management</td>
</tr>
<tr>
<td>ITSMF</td>
<td>IT service management Forum</td>
</tr>
<tr>
<td>MIA</td>
<td>Multidimensional Incident Analysis</td>
</tr>
<tr>
<td>MOF</td>
<td>Microsoft Operations Framework</td>
</tr>
<tr>
<td>MTO</td>
<td>Människa-Teknik-Organisation</td>
</tr>
<tr>
<td>NTSB</td>
<td>National Transportation Safety Board</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>PDCA</td>
<td>Plan-Do-Check-Act</td>
</tr>
<tr>
<td>RACI</td>
<td>responsible, accountable, consulted and informed</td>
</tr>
<tr>
<td>RCA</td>
<td>root cause analysis</td>
</tr>
<tr>
<td>SCM</td>
<td>Swiss Cheese Model</td>
</tr>
<tr>
<td>SCSI</td>
<td>Southern California Safety Institute</td>
</tr>
<tr>
<td>SECFC</td>
<td>simple events and causal factors chart</td>
</tr>
<tr>
<td>STAMP</td>
<td>Systems Theoretic Accident Modelling and Processes</td>
</tr>
<tr>
<td>UNEP</td>
<td>United Nations Environment Programme</td>
</tr>
</tbody>
</table>
LIST OF ORIGINAL PUBLICATIONS

This thesis is based on data presented in the following articles, referred to by the Roman numerals I–V.


The above publications have been included at the end of the printed version of this thesis with their copyright holders’ permission.
AUTHOR’S CONTRIBUTION

The author of this thesis was the corresponding author with the most contribution to all the papers. In all of the papers, the co-author, Marko Jäntti, reviewed the papers and provided valuable comments and guidance. He helped with the structure of the papers and especially with the introduction, scientific methods and literature. Regarding Paper V, the third co-author, Mika Hujo, helped with the theory and the tools of the Bayesian Belief Networks (BBN) and he also reviewed the results.

The data used in the research papers consists of written major or medium incident reports. The data in the reports were enhanced with additional data collection described in the papers in methods section. The data were gathered in IT service management audit engagements by the author and the project team related to engagements. The author was in all the engagements responsible of the engagement, and the primary contributor in designing the data collection. The IT service provider helped in identifying additional data sources, especially persons for interviews. This gathered data formed the pool, which was used in all the papers.
Contents

1 Introduction .................................................................19
  1.1 Research motivation .................................................19
  1.2 Related frameworks .................................................20
  1.3 Problem ..................................................................23
  1.4 Questions ..................................................................24
  1.5 Goals .......................................................................25
  1.6 Target audience .....................................................25
  1.7 Scope and limitations ..............................................26
  1.8 Structure of the thesis ..............................................27

2 Related studies: Incident models ...........................................29
  2.1 About incidents ......................................................29
  2.2 Root cause ............................................................31
  2.3 Modelling of incidents .............................................33
  2.4 Linear/sequential models .........................................34
  2.5 Complex linear models and epidemiological models ......35
  2.6 Non-linear, systemic accident models........................39
  2.7 Software problem and defect management models ......41
  2.8 Current state on accident models in research and practice ...43
  2.9 Bayesian Belief Network (BBN) ..................................44

3 Research framework .......................................................49
  3.1 Proactive problem management ..................................49
  3.2 Incident models ......................................................54
  3.3 Incidents in IT and in other industries .........................57
    3.3.1 IT service incidents have a longer duration ..............57
    3.3.2 Fewer human errors in IT incidents .......................57
    3.3.3 The quality of IT incident reports is poor ..............58

4 Research phases and research methods ...............................61
  4.1 Research phases ......................................................61
  4.2 Case study method and data collection procedures ........64
4.3 Research with action research method ........................................... 67
4.4 Model design with design science method .................................... 68
4.5 Analysis ...................................................................................... 70
   4.5.1 Data analysis related to all papers ......................................... 70
   4.5.2 Analysis in individual papers ............................................... 71
4.6 Experiences gained ..................................................................... 73

5 How incidents happen – Incident root cause categories ............ 75
   5.1 Multidimensional analytics of incidents ..................................... 75
       5.1.1 Categories of root causes of IT service incidents ........... 76
       5.1.2 Towards more sophisticated incident analytics ........... 76
       5.1.3 Incident trend analysis and incident investigation .......... 78

6 Why incidents happen – The IT Incident Model ......................... 81
   6.1 Requirements for an IT Incident Model (IIModel) ..................... 81
   6.2 Construction of the IIModel ..................................................... 84
       6.2.1 The taxonomy .............................................................. 85
       6.2.2 Presentation of incident scenarios .................................. 86
       6.2.3 Presentation of probabilities ......................................... 88
   6.3 The IIModel and MIA in the proactive problem management framework ......................................................... 88

7 Summary of the papers ................................................................. 91
   7.1 Relationship of the research papers and IT Service Management ................................................................. 91
   7.2 Summary of papers .................................................................. 93
       7.2.1 Creating an ITIL-based Multidimensional Incident Analytics Method: A case study .................. 93
       7.2.2 Quality and Human Errors in IT Service Infrastructures - Human Error Based Root Causes of Incidents and Their Categorisation ..................................................... 94
       7.2.3 A Case Study on the Improvement of the Incident Investigation Process ........................................... 95
       7.2.4 The Anatomy of IT Service Incidents .............................. 96
       7.2.5 A model for analysing information systems incidents: A proactive approach .......................... 96
1 Introduction

Information technology (IT) service providers are constantly seeking more effective methodologies, processes and tools to optimize the efficiency and quality of service management processes. The key challenge in many IT service provider organisations is that they operate their support services in an overly reactive mode. They focus too much on reacting to already reported incidents, instead of taking proactive measures for preventing their future occurrence. Understanding how incidents emerge and what their root causes are, is fundamental to establishing proactive measures to prevent incidents from occurring and reoccurring.

The IT Infrastructure Library (ITIL) (Office of Government Commerce 2011b) is the most widely used IT service management framework. It provides a set of guidelines and processes for managing IT infrastructure, design, and operations. It also addresses the quality of IT services in several different ways. The most important quality process areas within IT service management (ITSM) are service level management, incident management and problem management processes and the continual service improvement (CSI) stage of the IT service lifecycle. IT service quality also plays major role in availability management, capacity management, and IT service continuity management processes.

1.1 RESEARCH MOTIVATION

Virtually all functions of modern society are dependent on IT services, their uninterrupted operation and their high quality. The cost of IT service incidents is high; IT downtime cost was 700 billion USD annually (2015) to North American companies. This cost is primarily composed of the loss of employee productivity
IT service incident costs totalled 4% of the combined gross domestic product (GDP) of the United States and Canada (International Monetary Fund 2015). Ponemon Institute has stated that an outage in a data centre costs, on average, 8000 USD per minute; the average overall cost per incident is 630,000 USD (Ponemon Institute Research Report 2013). Thus, mitigating the number and impact of IT service incidents is of extreme importance at the organisational and national level.

Knowledge of the underlying factors, events and conditions leading to an incident creates the basis for proactive measures to prevent incidents from occurring and reoccurring. Compared to other industries, there has been very little research on incident models within the ITSM, especially taking into account the special features of IT, which are identified in this thesis. Accident investigations and accident models in the other industries have a long history of over two hundred years (Klein 2009). Many studies have been conducted in industries where accidents result in casualties (e.g. aviation, maritime, railway, healthcare, pharmaceutics, nuclear energy, and the chemical industry) (Saarelainen, Jäntti 2016).

1.2 RELATED FRAMEWORKS

In this section, the major ITSM and IT governance frameworks are presented. Problem management is a key process in ITSM. Hence, the focus in this thesis is on problem management. After the general introduction of the framework is conducted, the problem management is presented.

The most notable ITSM frameworks include ITIL, ISO/IEC 20000 and COBIT. These all share the same roots, terminology, family resemblances and compliance (Fig. 1). Problem management is described and discussed in all of these frameworks.
ITIL provides a set of guidelines for managing IT infrastructure, development, and operations. ITIL also addresses the quality of IT services in several different ways. The ITIL 2011 edition is the current form of ITIL. It is the revised version of ITILv3, which, in turn, is derived from ITILv2, but includes major changes.

In this thesis, ITIL refers to ITIL 2011 Edition. ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage: Service Strategy, Service Design, Service Transition, Service Operation, and CSI. Each of the lifecycle stages consist of a number of ITSM processes. Altogether, there are 26 processes with four supporting functions (Office of Government Commerce 2011a). In this thesis, the primary focus is on problem management, as ITIL describes it. It is one of the processes of the service operation stage of the lifecycle.

ISO 20000: ITIL provides best practices and guidance on how to implement IT Services to support the business processes of customers. ITIL qualifications are available for individuals; however, an IT organisation cannot easily prove that it is working along the ITIL recommendations.

The ISO/IEC 20000:2011 standard (abbreviated to ISO 20000 in the rest of this publication) (ISO/IEC JTC 1, SC 7 2011, ISO/IEC JTC 1, SC 7 2005) was initiated by the ITSM Forum (ITSMF) and British Standards Institution (BSI) to fill this gap. It is modelled upon the principles of ITIL and allows IT organisations to have their ITSM certified. In contrast to the ITIL books, ISO 20000 does
not offer detailed descriptions on how to implement the ITSM processes. It is rather a set of requirements which must be met to qualify for ISO 20000 certification (e.g., “the service provider shall analyse data and trends on incidents and problems to identify root causes and their potential preventive actions”) (ISO/IEC JTC 1, SC 7 2011). Fig. 2 illustrates the ISO 20000 requirements and processes at a higher abstraction level, as compared to ITIL.

Control Objectives for Information and Related Technology 5 (COBIT 5) (ISACA 2012) is a framework created by Information Systems Audit and Control Association (ISACA) for IT management and IT governance. COBIT 5 covers 37 processes in five domains: Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA).

The process set of COBIT is oriented more to an IT organisation of an enterprise, rather than towards an IT service provider. The process Manage problems (DSS03), defines IT-related goals with related metrics, a responsibility table (RACI chart), and process practices, inputs/outputs and activities.

COBIT describes both inputs and outputs. Some examples of inputs are risk-related root causes, criteria for problems, problem logs, incident resolutions, closed service requests and incidents. Examples of outputs are problem classification scheme, problem
status reports, problem register, root causes of problems, problem resolution reports, known-error records, proposed solutions to known errors, closed problem record, communication of knowledge learned, problem resolution monitoring reports, as well as identified sustainable solutions. The process descriptions in COBIT 5 are formal and make for very compact table format presentations. E.g. the problem management process in COBIT is defined in three pages, while in ITIL, it is defined in 13 pages.

**Business Process Framework (eTOM)** (ITU-T Study Group 4 2007a, ITU-T Study Group 4 2007b) is a process framework for telecommunications service providers in the telecommunications industry maintained by the TM Forum. The model describes the required business processes, including the ITSM processes of service providers, and defines the key elements and their interactions.

eTOM consists of a hierarchy of four process levels of increasing amount of details. IT related processes are, in practice, often replaced by ITIL processes by telecommunications service providers. The reason for this is that communications services are part of virtually any IT services, where ITIL is the most popular ITSM framework.

### 1.3 Problem

Despite the financial impact and the importance to society and daily life, few academic IT service incident studies have been conducted. There is an apparent gap in current knowledge regarding understanding how and why IT service incidents emerge, what are their preceding events, conditions and contributing factors. The research problem of this thesis is the lack of models or frameworks for managing incidents.
1.4 QUESTIONS

The research question in this thesis is:

What tools, methods, practises and aspects should be included in the model for IT service incidents?

To address this research question, the following additional research questions were formulated:

1. How do incidents happen and how should the root causes of incidents be categorized?

2. Why do incidents happen and what events and conditions cause or increase the probability of an IT service incident?

3. What events or conditions during an IT service incident lengthen its duration or increase the impact of it?

4. How could the incidents in the ITSM operating environment be modelled to aid proactive problem management, root cause analysis and CSI?

The first research question creates the basis for the incident trend analysis. One of the key objectives of the incident categorisation activity is to provide information for identifying the same type of incidents caused by the same root cause. An incident trend analysis is part of proactive problem management. It refers to an analysis of historical incident records to identify one or more underlying causes that, if removed, can prevent their reoccurrence (Office of Government Commerce 2011c). Thus, an incident trend analysis can be seen as part of the CSI process (Office of Government Commerce2011a, Office of Government Commerce2011b).

The second research question goes beyond listing the most frequent root causes by investigating the underlying events and conditions contributing to the incident. Preventing the reoccurrence of incidents is conducted by removing or changing these contributing events and conditions.

The motivation behind the third research question is that IT service incidents have a duration, unlike incidents in many other industries. The impact of an IT service incident is also proportional to the length of it. Any events or conditions which
prolong restoring the service can be considered adverse in the same manner as the incidents itself.

The aim of the fourth research question is to construct a comprehensive incident model, where all entities, parameters with their values and relationships could be placed. This model acts as a tool and a framework in an incident investigation. If the incident and its contributing events, with their probabilities, are modelled mathematically, the model has the ability to predict the probabilities of the upcoming events. This model, if proven effective, can also be used as a tool in proactive problem management.

The results of this research can be used directly in the problem management process in incident investigations and in proactive problem management. The results also benefit from all of the aforementioned processes and stages of the service lifecycle.

1.5 GOALS

The short-term goal of this research is to develop an IT incident model with practical methods and tools for incident investigation, trending and prediction. The long-term goal is to extend the knowledge in this area, explore why IT service incidents happen and determine the contributing factors behind them.

1.6 TARGET AUDIENCE

This thesis has two main target audiences: the IT industry and academia.

Regarding the IT industry audience, the primary target are the IT service management roles related to incident and problem management and service improvement. Incident and problem management process owners may consider modifying corresponding processes according to findings presented in this thesis. In fact, some of the results may be useful in the future
version of the book “ITIL Service Operation” in a new chapter describing proactive problem management process. Incident and problem managers and problem analysts will find useful tools and methods in their daily work in this thesis. Roles related to quality and continual service improvement, e.g., CSI managers, service level managers and quality managers, may gain access to useful tools and input for their activities.

Regarding academia, the proposed IT incident model challenges existing incident models, brings out the different nature of IT service incidents compared to other industries and, in general, increases understanding of the causes and contributing factors of IT service incidents.

1.7 SCOPE AND LIMITATIONS

The results of this study contribute mainly to the ITIL problem management process, and thereby proactive problem management. The results will be useful in incident management and especially in the incident investigation phase.

There are certain limitations to the research. The number of incident reports available was only somewhat over 200 reports. The research in this thesis is made in five publications. Depending of the publication, a smaller subset of these reports was used. The low number of incident cases results in lower statistical accuracy. Second, the reports were made by a certain IT service provider, which may not provide a representative picture of the entire industry, although there were several separate and different environments throughout the reports. Environments where incidents were collected did not cover all the typical areas in IT services. For example, there were no incident cases in cloud services or end-user support. The limitations of the case study research method include the possible biased views of the researcher. This was mitigated by using two researchers, multiple data sources and confirmation and/or discussion of the conclusions with the interviewees.
1.8 **STRUCTURE OF THE THESIS**

This thesis consists of five research papers; this summary is comprised of eight chapters.

Chapter 2 contains the literature review and related work conducted in the field of accident and incident investigations and modelling.

Chapter 3 identifies the frameworks, which present two viewpoints: proactive problem management and incident investigation.

Chapter 4 presents the research phases, research methods, data analysis as well as experiences gained during the research.

Chapter 5 presents the root cause categories of incidents, in general. It opens up the role of human errors as a root cause. The chapter also introduces the methods and good practices for a root cause analysis. This chapter is based on the research conducted in Papers I, II and III.

Chapter 6 introduces the incident model related to the root causes and the extended model of the incident lifecycle. This model is then adapted to a Bayes network of conditional probabilities with a set of real life incidents with their relationships and probabilities. This chapter is based on the research in Papers IV and V.

Chapter 7 presents the summaries of the original publications (Papers I-V), while the original research articles are included at the end of the printed version of this thesis.

Chapter 8 summarizes the study and presents ideas for future research.
2 Related studies: Incident models

In this section, the related studies and literature in the area of accident and incident investigations is explored. The different flavours of incidents and the essence of the root cause are discussed. The development of incident models are then discussed and the major models used in practice and in science are presented. This existing work will used later in construction of the IT incident model.

2.1 ABOUT INCIDENTS

The tradition of incident investigation begins with an accident investigation, where the harmful events are likely to cause injuries or casualties. These events are typically called disasters, accidents, incidents, mishaps, near misses, dangerous occurrences and undesired circumstances, depending on the magnitude of the impact. From the business point of view, incidents are different levels of harm from an increased probability of service breaks or a reduced quality of service to business breaks and disasters.

The incident management process in ITIL classifies incidents in order to apply appropriate processes or procedures to them. Different types of incidents in different contexts are presented in Fig. 3.
Incidents can be considered one class of the outcomes of events. It is a variation of the normal operation (Fig. 4). The severity and impact of the incidents is variable. The incidents are usually prioritized by logging according to impact and urgency. The range of incidents and incident priorities is extensive. Some low impact incidents may be treated or even classified as a service request, even though they fulfill the characteristics of the incident definition (e.g., lost passwords or a lack of ink in the printer).

The failure of a configuration item that has not yet affected a service is also an incident (e.g., failure of one disk from a mirror set) (Office of Government Commerce 2011c). These are usually handled by the request fulfilment process.

On the other end, disasters, an extreme type of incident, are managed by the ITIL IT service continuity management process, not by the incident or problem management. Incidents with low business impacts are handled by the request fulfilment process.

In this thesis, the word “incident” covers all types of adverse events.

Hollnagel (Hollnagel 2010) presented the attributes related to events (e.g. nature of outcome or impact (negative – positive), predictability (very low – very high) and frequency). Notice that there also may be planned negative effects caused by changes in the form of planned service breaks. However, incidents are unplanned events, unlike changes, which are planned. Since incidents are unplanned, they have a negative outcome.
The frequency of incidents is also smaller than the frequency of normal operational transactions. The different flavours of events with these parameters are presented in Fig. 4. The basic idea from Fig. 4 was developed by Hollnagel (Hollnagel 2010), while the positioning of the events related to IT services was developed by the author.

2.2 **ROOT CAUSE**

There is no widely accepted definition of root cause. Root cause, however, plays a key role in this thesis. Most outcomes are built on the assumption that a root cause has certain characteristics. Thus, it is essential to have a precise definition, which is in line with most of the available practices, studies and documentation.

ITILv3 2011 edition defines root cause as (Office of Government Commerce 2011c): “Root cause is the underlying or original cause of an incident or problem”. This definition indicates that the removal of the root cause will prevent similar incidents or problems from reoccurring.

The root cause definition from the United Nations (United Nations Environment Programme (UNEP) 2010) and OECD
(OECD2003) addresses the prevention of accidents: “The prime reason that leads to an unsafe act or condition and results in an accident or near miss. In other words, a root cause is a cause that, if eliminated, would prevent the scenario from progressing to an accident.” An unsafe act is mentioned in the domino model and in the Human Factors Analysis and Classification System (HFACS).

According to Paradies (Paradies, Unger 2000), the root cause is “the most basic cause (or causes) that can reasonably be identified that management has control to fix and, when fixed, will prevent or significantly reduce the likelihood of the problem’s reoccurrence.” This definition links the concepts of the root cause and the problem, which are among the key principles in IT service problem management.

The father of the Swiss Cheese Model (SCM) allows for several underlying causes: “Root cause is the contributing factor that you are working on when the money or the time runs out.” (Reason, Hollnagel & Paries 2006). In the SCM model, which is used in this study, there may be several latent failures contributing to the active failure.

Corcoran (Corcoran) has collected 50 different definitions of root cause from various sources. 30% of the definitions allowed for only one root cause; 68% permitted several root causes. In 56% of the root cause definitions, corrective actions prevented the reoccurrence of a problem. 16% of the corrective actions reduced the probability of reoccurrence. Several root causes are not only allowed, they are also required in all of the incident models to be presented later.

Paper II presents the following definition of root cause: “Root causes are the underlying causes of an incident or a problem, which if corrected would prevent or significantly reduce the likelihood of the incident’s reoccurrence.” This definition plays an important role, because it allows for several root causes. Corrective actions either prevent or significantly reduce the probability of reoccurrence. These corrective actions include the standardisation of devices, using fault tolerant designs, setup monitoring, automate, improve/correct processes, work instructions, and their supervision. This definition leaves space to the inaccurate
Related studies: Incident models

judgment of the root cause analyst and the dynamics of complex relationships between the actors in an ITSM environment. The definition is compatible with the incident model used in this study. It also refers to the incidents and problems, as defined in the ITIL framework.

2.3 MODELLING OF INCIDENTS

Incident models provide a conceptualisation of the characteristics of the incident, which typically show the relationship between the causes and effects. They explain why accidents occur. They may be used as techniques for risk assessment during system development or in prioritisation of the improvement activities, in incident investigations and in an incident trend analysis.

Incident causation has been widely studied over the past 200 years to explain and prevent their occurrence. This is especially the case in industries where the incidents are either lethal or very expensive. These industries include aviation, energy, health care, transportation, maritime, railways, mining and chemical industries and the military (Ergai 2013).

The number of different models and theories is overwhelming. Stanton (Stanton et al. 2006) lists over 100 incident models related only to human factors. The research field of incident investigations is shared by psychologists, statisticians, managers and engineers. This thesis follows the categorisation of incident models used by the mainstream of incident model research (Reason, Hollnagel & Paries 2006, Toft et al. 2012, Qureshi 2007, Griffin, Young & Stanton 2015). In this thesis, the main categories of the incident models have two names, since the terminology varies in different sources. Most of these models represent the psychological research tradition. This is a natural approach, since across almost all of the industries, human errors are the most common root cause of accidents, as will be shown later.

In this section, only the most visible models in the recent literature are presented, because of the huge number of models. In fact, one objective of this research is to add one model to this
crowd, because the existing models do not adequately fit in the ITSM practices.

Possibly the earliest well documented effort to study incident causation knowledge is that of the Du Pont company founded in 1802. According to Klein (Klein 2009), the company founder, E.I. Du Pont (1772 – 1834), once noted that “we must seek to understand the hazards we live with”. The design and operations of Du Pont’s explosive factories were gradually improved to better understand how catastrophic explosions were caused and could be prevented.

2.4 **LINEAR/SEQUENTIAL MODELS**

In the 1930’s, William Herbert Heinrich, an employee working for Traveller’s Insurance Company, published Industrial Accident Prevention in 1931 (Heinrich 1931), This publication is the first major work in understanding and modelling incidents (Toft et al. 2012).

Heinrich explained the incident as a causal chain, sequence of events, and a natural culmination of a series of events of circumstances, which occur in a specific order (Fig. 5). According to this **domino model**, incidents may be prevented by removing one of the dominos, and thus, interrupting the knockdown effect. Heinrich focused on the human factors, which he termed “Man Failure”, as the cause of most incidents.

![Figure 5. Domino theory sees the accident as result of a sequence of events (Heinrich 1931).](image-url)
Sequential models focus on the view that incidents happen in a linear way, where A leads to B, which leads to C. Hence, they examine the chain of events between multiple causal factors displayed in a sequence. Incident prevention methods focus on finding the root causes and eliminating them, or putting in place barriers to encapsulate the causes.

A straightforward sequential domino theory was later enhanced by many additional features. Bird (1974) updated the domino theory by adding one domino with the organisational perspective (Bird 1974). This theory was, in turn, enhanced by Weaver, with the role of the management system (Griffin, Young & Stanton 2015).

In his multiple causation model, Petersen stated that there are two major features of events which lead to an incident: an unsafe act and an unsafe condition (Stranks 2007).

### 2.5 COMPLEX LINEAR MODELS AND EPIDEMIOLOGICAL MODELS

Complex linear models explain the incident as an outcome of the combination of active failures (unsafe acts) and latent conditions (hazards) that existed together at the time of incident. Reason (Reason 1990) adopted the epidemiological metaphor in presenting the latent contributing factors as ‘resident pathogens’. As in the epidemic of infectious diseases, the hosts (e.g. human actor of potential accident) with different levels of intrinsic physical physiological immunities are exposed to these latent conditions in various physical, psychological and social environments (Toft et al. 2012).

One of the best known incident models is Reason’s Swiss Cheese Model (SCM) (Reason 1990). It explains the role of the human factors incident. According to SCM, the incident is the result of long standing conditions and latent failures, contributing to the unsafe act. The model is usually described as a sequence of planes (e.g. slices of cheese), which describe the organisational levels, defences and barriers.
Failures (holes in the slices of cheese) can emerge at any of these levels. When the holes are simultaneously in the same trajectory, the incident is likely to occur.

The most common application of the SCM is the Human Factors Analysis and Classification System (HFACS) (Wiegmann 2001). It has a multilevel taxonomy for active human errors (“unsafe acts”) and latent conditions contributing to the unsafe act. HFACS splits different human errors into four main failure layers, or “slices of Swiss cheese” (Fig. 6): 1) Organisational factor influence; 2) daily management or supervision. Failures in supervision produce; 3) preconditions, which eventually lead to; 4) acts causing the incident (Fig. 7). The HFACS is, in some sources, categorised as a systemic model (Salmon, Cornelissen & Trotter 2012).

The HFACS has its origin in aviation accident investigations. However, there have been many adaptations to it in a variety of industries (e.g. aviation (Shappell, Wiegmann 2001), aviation maintenance audit (Hsiao et al. 2013), aviation maintenance (Boex 2001), air traffic control (Pounds, Isaac 2002), U.S. Marine Corps (Bilbro 2013), manufacturing (Olsen, S. T. Shorrock, S. T. 2010). The HFACS is also widely used in the military (e.g. USA, Canada, Australia) (Department of Defence 2005), U.S. Forest Service (Pounds, Isaac 2002), U.S. Coast Guard (Pounds, Isaac 2002), biopharmaceuticals (Cintron 2015), railroads (Reinach, Viale...
Related studies: Incident models

2006). Additionally, the HFACS has gained interest in containerized dangerous cargoes (Ren 2009), mining (Patterson 2009), security (Wertheim 2010) and construction (Garrett, Teizer 2009).

There are also other models based on the SCM, which have not gained that much popularity and are often industry or even country specific. Examples of these include the Human Error in European Air Traffic Management (HERA) and the Australian Transport Safety Bureau (ATSB). HERA is used in air traffic control (Griffin, Young & Stanton 2015). It can be considered an alternative or complimentary model and methodology to HFACS. ATSB is used in Australian railways (Baysari, McIntosh & Wilson 2008).

Events and causal factors chart (ECFC) (DOE 1999, Buys, Clark 1995) is a graphical presentation of the chronology of the incident. It is used primarily for compiling and organising evidence to present the events and conditions leading up to an incident. ECFC consists of the primary events sequence, secondary events sequence and the conditions influencing the events.

Figure 7. The hierarchical HFACS taxonomy of human factor contributions on incidents and accidents (Shappell, Wiegmann 2001).
The primary sequence of events leading up to an accident is drawn horizontally in chronological order from left to right. Secondary events and conditions are above the primary sequence line. “Presumed” events and conditions may also be described in the chart, marked as dotted lines (Fig. 8).

**MTO (Människa–Teknik-Organisation), aka the HTO model (Human-Technology-Organisation),** considers human factors, technology, and organisations to have equal importance in incidents (Rollenhagen 1995). MTO can present an incident as an outcome of complex interactions and coincidences, because of the normal performance variability of the system, rather than the actual failures of the components or functions.

MTO is an industry independent model. The MTO-analysis is based on three methods (Figure 9):

- Structured analysis by use of an ECFC;
- Change analysis by describing how events have deviated from earlier events or common practice;
- Barrier analysis by identifying technological and administrative barriers, which have had failures or are missing.

MTO describes the direct cause relationships in a versatile and many-sided way. Some sources, however, categorize MTO as systemic accident model (Reason, Hollnagel & Paries 2006). MTO and ECFC will contribute to the structure of the IT Incident Model developed in this thesis.
2.6 **NON-LINEAR, SYSTEMIC ACCIDENT MODELS**

The contemporary view of accidents is that accidents are not due only to active failures, but also to normal variations in a connected complex system. According to the systemic accident models, it is unadvisable to describe the cause-effect relationships of accidents within a complex system (Hollnagel 2009, Dekker 2012).

Systemic models are popular among researchers, but lack support in the incident investigation practitioners’ community (Underwood, Waterson 2014). These are, however, presented here to build a comprehensive picture of the incident models, in general, and to understand why certain models and features are not included in the IT Incident Model.

**Functional Resonance Accident Model (FRAM)** by Erik Hollnagel graphically describes systems as a network of interrelated sub-systems and functions. The performance variability of any given system component can “resonate” with the remaining components and result in an incident.

![Figure 9. Människa–Teknik-Organisation (MTO) diagram used in incident investigation (Rollenhagen 1995).](image)
In a FRAM diagram (Fig. 10), the main focus is on the interaction of system components and the associated effects between them (Hollnagel 2012, Hollnagel 2004). FRAM requires modelling of the entire system, which is too time consuming for the IT investigator’s fast paced work.

**Systems-Theoretic Accident Model and Process (STAMP)** proposed by Leveson considers system safety as a continuous control task to impose the constraints necessary to limit the system behaviour to ensure that there are only safe changes and adaptations (Leveson 2004). This accident model is aimed at determining why the controls failed to detect or prevent changes that ultimately lead to an accident. STAMP is either used or known within researchers, but practically non-existent as the tool of practitioners (Underwood, Waterson 2013).

**Accimap** method is based on Rasmussen’s risk management framework (Rasmussen et al. 2010, Rasmussen 1997). It focuses on failures across the following six organisational levels: 1) government policy and budgeting, 2) regulatory bodies and associations, 3) company management, 4) technical and operational management, 5) physical processes and actor activities, and 6) equipment and surroundings (Fig. 11).

Accimap is a generic approach. It does not use taxonomies on the causes or contributing conditions. The AcciMap approach involves the building of a multi-layered causal diagram.
Accimap models the full range of factors and causes up to the event. The most immediate causes are shown in the lower sections of the diagram; the more remote causes are shown at progressively higher levels.

There is no taxonomy in Accimap (Salmon, Cornelissen & Trotter 2012, Underwood, Waterson 2014). The hierarchical framework is useful in IT services, although the structure is much simpler in an IT environment with a much narrower scope.

2.7 SOFTWARE PROBLEM AND DEFECT MANAGEMENT MODELS

A defect is defined by the Institute of Electrical and Electronics Engineers (IEEE) “as any unintended characteristic that impairs the utility or worth of an item, or any kind of shortcoming, imperfection, or deficiency” (IEEE1988). Currently, there are two main approaches that IT organisations may use to assure quality and manage defects and problems: 1) traditional software quality assurance (including defect management) and 2) service-oriented
quality assurance (including problem management) (Jäntti 2008). The latter has gained popularity, because focus in IT organisations has been shifted from software products towards services. Today’s IT managers emphasize service quality in favour of product quality.

The IEEE Standard Classification for Software Anomalies (IEEE Std 1044-2009 2010) defines anomalies as problems and defects found during the review, test, analysis, compilation, or use of software products or documentation (Table 1). These activities represent different phases in the lifecycle of a software product. This activity list is equivalent to the ITSM service lifecycle stages presented in ITIL.

The stages of an IT service lifecycle include service strategy, design, transition, operation and CSI. The defect areas in customer service (Table 1) are directly related to the ITIL service operation (e.g. operation procedures, maintenance updates, and support documents) and service transition (e.g. installation procedures) stages of the IT service lifecycle. The similarity of product development and service development lifecycles encourages further deployment of the same problem management processes as with other IT services.
Related studies: Incident models

Table 1. Problem and defect finding activities (Florac 1992).

<table>
<thead>
<tr>
<th>Activities</th>
<th>Find problems in software management</th>
<th>Find problems in IT service management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product synthesis</td>
<td>Requirement specs, Design specs, Source code, User publications, Test procedures</td>
<td>Application management specs and processes</td>
</tr>
<tr>
<td>Inspections</td>
<td>Requirement specs, Design specs, Source code, User publications, Test procedures</td>
<td>Reviews and inspections of service documents, records and configuration items</td>
</tr>
<tr>
<td>Formal Reviews</td>
<td>Requirement specs, Design specs, Implementation, Installation</td>
<td>Reviews and inspections of service documents, records and configuration items</td>
</tr>
<tr>
<td>Testing</td>
<td>Modules, Components, Products, Systems, User publications, Installation procedures</td>
<td>Release testing, Service evaluation</td>
</tr>
<tr>
<td>Customer Service</td>
<td>Installation procedures, Operating procedures, Maintenance updates, Support documents</td>
<td>Incident management procedures, Service desk documents, User manuals of services</td>
</tr>
</tbody>
</table>

2.8 CURRENT STATE ON ACCIDENT MODELS IN RESEARCH AND PRACTICE

According to Salmon (Salmon, Cornelissen & Trotter 2012) three causalisation models dominate the current incident model literature: 1) Rasmussen’s risk management framework and its Accimap method, 2) Leveson’s Systems Theoretic Accident Modelling and Processes Model (STAMP) and 3) Reason’s omnipresent Swiss Cheese model; especially its taxonomy based
analysis approach, the Human Factors Analysis and Classification System (HFACS), by Shappel and Wiegmann (Salmon, Cornelissen & Trotter 2012).

The author would like to add a fourth member to this group, namely Hollnagel’s Functional Resonance Accident Model (FRAM), which is visible in the literature in relation to the comparisons of various models (Underwood, Waterson 2014, Underwood, Waterson 2013).

Underwood and Waterson studied the popularity of various incident models among practitioners and researchers (Underwood, Waterson 2014). They conducted a study about the awareness and usage of STAMP, FRAM, Accimap, the Swiss Cheese Model (SCM) and the Fault tree models among incident investigation researchers and practitioners. The researchers were, in general, familiar with all of the models. The results revealed that Fault Tree and SCM were the most popular. The practitioners, however, had not used most of the systemic models (i.e. STAMP, FRAM and Accimap). One observation in the study was that the practitioners and research communities communicated very little.

Additionally, Underwood and Waterson applied STAMP, Accimap, and the SCM-based ATSB model (the Australian Transport Safety Bureau) to a well-known railway accident (Underwood, Waterson 2014). The results illustrated that ATSB was best suited for practitioners and STAMP was best suited for researchers, while AcciMap may more easily meet the needs of both parties.

2.9 **BAYESIAN BELIEF NETWORK (BBN)**

A BBN is a probabilistic graphical model (a type of statistical model) that represents a set of random variables and their conditional dependencies/independencies. The variables are presented as nodes. The dependencies/independencies are presented by the structure of the network. The structure is called
a directed acyclic graph (DAG), graphically described by arrows between the nodes. In DAG, no loops are allowed in the structure.

BBN is based on Bayes’ theorem, stated mathematically as the following equation:

\[ P(A|B) = \frac{P(A) P(B|A)}{P(B)} , \]

where:

- A and B are events.
- P(A) and P(B) are the probabilities of A and B being independent of each other.
- P(A|B), a conditional probability, is the probability of observing event A, given that B is true.
- P(B|A) is the probability of observing event B, given that A is true.

The Bayesian Belief Network (BBN) is not an accident model, but it is well suited to describe incidents, events and conditions, as well as the relationships and probabilities between them. Conditional probabilities may be obtained automatically from the data, or they can be the input of experts or a combination of these two; for example, in the BBN of a computer system, relationships may be modelled by an expert (“if server A is down, servers B and C are down”). The probabilities of server downtime may be taken from the incident or service level statistics. The relationships may also be read from the configuration management database (CMDB). The server failure probabilities may be the result of the educated guess of an expert.

This example of modelling an IT incident by the BBN shows how the framework is applied to a typical small incident (e.g., the personal printer does not print). The example is further simplified by limiting the number of the root causes to three. There is simply no paper in the printer, which is possibly contributed to by an unexperienced user, who does not notice the lack of paper. If the paper is not finished, then the incident is covered by another root cause, which covers all the other failures.
Figure 12. A Bayesian Belief Network (BBN) of a simple printer incident with two potential direct root cause categories and human error as a contributing factor. The probability calculation of the BBN is governed by the conditional probability tables.

The root causes, with their initial probabilities, are presented in Fig. 12. If somebody calls the service desk and reports that the printer does not print, the corresponding probability in the BBN is now set to 100%, since we now have evidence that the printer does not print. In this case, the service desk also knows that the user is unexperienced and that probability can also be set to 100%. The conditional probabilities are calculated and the most probable root cause, in this case, is the lack of paper. Introduction to Bayesian networks and the examples in Figs. 12 and 13 are presented in Paper V.
Failure probability has been studied by Zhang et al. (Zhang et al. 2009, Zhang, Pham 2000) who proposed a model of service availability that uses event management logs and incident records to assess the failure probability and configuration management data base (CMDB) relationships for building a BBN. Using existing data, it is possible to at least partially automate the incident analysis process. The model is used to estimate the expected probability of, and duration of, the failure.

Deng et al. (Deng et al. 2014) proposed a manually maintained datacentre meta-model, populated by actual CMDB and topology discovery tools. The virtual part of the model is modelled as a Bayesian network.

Franke et al. (Franke, Johnson & König 2014, Franke et al. 2012) made a predictive model for availability purposes. Factors affecting the availability are captured in Marcus and Stern (Marcus, Stern 2000). These factors are validated, and their probabilities are estimated, by an interview of 50 availability experts.

Wang et al. (Wei Wang et al. 2013) developed a BBN-based integrated model for problem determination and change impact analysis. The model is built by experts, with the help of data from the CMDB, and event log files. Nadi et al. (Nadi et al. 2009) combined CMDB relationships, time information from incident reports, and change history in a causal graph. The result is a semiautomatic system for root cause and change impact analysis.

Hinz and Gewald (Hinz, Gewald 2006) studied latent factors contributing to IT infrastructure risks with a desktop focus using expert interviews. Experts were interviewed about the risks and
their causal relationships, which were modelled in a Bayesian Belief Network. Steinder and Sethi (Steinder, Sethi 2004) applied the BBN in the fault location in communications.

Marsh and Bearfield used BBN networks to model accident causation in the UK railway industry (Marsh, Bearfield 2004).
This thesis synthesises existing work and frameworks in ITSM with incident investigation results from other industries and disciplines. In this section, the research framework is described from the two major viewpoints.

The first viewpoint is proactive problem management in the context of ITSM. Proactive problem management is augmented by a generic incident investigation process. These are presented as part of continual service improvement processes.

The other viewpoint is the incident model in the context of incident investigation. Most incident models are built on psychological research. More profound information of the topics here are presented in Section 2 of the related studies. The current relevant incident investigation practises in ITSM and the special features in IT incidents are presented.

3.1 PROACTIVE PROBLEM MANAGEMENT

According to ITIL (Office of Government Commerce 2011c) problem management is “the process responsible for managing the lifecycle of all problems. Problem management proactively prevents incidents from happening and minimizes the impact of incidents that cannot be prevented.” The first part of the definition refers to proactive problem management. The latter part of the definition refers to reactive problem management.

Reactive problem management is concerned with solving problems in response to one or more incidents. Proactive problem management tries to identify problems that might otherwise be missed. Proactive problem management analyses incident records. It also uses data collected by other ITSM processes to identify trends or significant problems.
The most important activities in proactive problem management are incident trend analysis and major problem review (Office of Government Commerce 2011c). The major activities in problem management are presented in Fig. 14; these include the inputs and outputs to these activities. Those parts, which are in the scope of this thesis, are marked in red text.

An IT service incident is, by definition, “an unplanned interruption to an IT service or reduction in the quality of an IT service.” A problem is “a cause of one or more incidents”. According to ITIL, one does not know the root cause, when the problem record is created. Problem management carries out the investigation of the root cause. The incident management process is “responsible for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized.”

The following example describes the differences between these terms:

- The server hangs up (incident).
- The server is booted to get the service up and running (incident management).
- A separate investigation is conducted (problem management)
- It was determined that there is a shortage of memory space (root cause).
- In regular review of problem reports, it is noted in the incident that there are a reoccurrence of similar
incidents in certain groups of servers with the same root cause (proactive problem management). The problem management process flow is presented in Fig. 15. A close relationship exists between proactive problem management activities and CSI lifecycle activities that directly support identifying and implementing service improvements.
Proactive problem management supports those activities through incident trend analysis and the targeting of preventive actions (Office of Government Commerce 2011c).

The ITIL CSI uses a closed loop feedback system, Plan-Do-Check-Act (PDCA) cycle, aka the Deming cycle. The Deming cycle is a fundamental element of CSI. It is also visible in many quality standards and reference books, including ITIL (Office of Government Commerce 2011a) and ISO/IEC 20000 (ISO/IEC JTC 1, SC 7 2011, ISO/IEC JTC 1, SC 7 2005).

The PDCA cycle is critical at two points in CSI: the implementation of CSI and the application of CSI to services and service management processes. The seven-step improvement process in CSI can be viewed as an example of an implementation of the PDCA cycle, with each of the steps falling within one of the phases of the cycle: Plan, Do, Check, Act.

The process flow in Fig. 15 only describes reactive problem management. There is no process flow description of the proactive problem management. Proactive problem management is seen in this process diagram as one source of inputs. Proactive problem management is triggered by an incident trend analysis, major problem review or other quality activities, which result in the need to raise a problem record, and in many cases, a request for change to resolve the problem.

To establish a more detailed framework of proactive problem management for this thesis, a more detailed description was prepared of the key activities in proactive problem management. Incident investigation processes are discussed in Paper II. The generic incident investigation process by European Safety Reliability and Data Association (ESReDA) (ESReDA Working Group on Accident Investigation 2009) with its iterative approach, is adopted as a framework for the incident investigation in this thesis (Fig. 16). ESReDA is a non-profit association of European industrial and academic organisations concerned with advances in the safety and reliability field.
The ESReDA process is suitable for an original incident investigation, major problem review and for an incident trend analysis as a one-time exercise. The ITIL, however, presents incident trend analysis as a periodic, scheduled activity. On the other hand, the PDCA and the seven step improvement process are described as fundamental principles in CSI. By adding two steps to the ESReDA process, it becomes fully compliant with the seven step improvement process. The added steps, in this case, are to implement recommendations and risk assessments. Fig. 17 shows the PDCA cycle, the seven step improvement process and the ITIL-based proactive problem management with the ESReDA incident investigation process. This proactive problem management process can be used in an incident trend analysis and major problem reviews.
3.2 INCIDENT MODELS

The Swiss cheese model (Reason, 1990) and its most common application, Human Factors Analysis and Classification System (HFACS) (Wiegmann 2001), was used as starting point in the development of the IT Incident Model. Människa–Teknik–Organisation (MTO) (Rollenhagen 1995) and Accimap (Rasmussen et al. 2010, Rasmussen 1997) also contributed to the IT Incident Model. These models can be categorized as complex linear models, epidemiological models and non-linear, systemic incident models. These incident models are discussed in more detail in Section 2.

An ITIL incident model is defined in the service operation stage of the service life cycle. However, the word “model” has different a meaning in different contexts. According to ITIL, an incident model “is a way of predefining the steps that should be taken to handle a process in an agreed way.” Additionally, ITIL defines a procedure as “a document containing steps that specify how to achieve an activity. Procedures are defined as part of processes”. Process, in turn, is defined as “a structured set of activities designed to accomplish a specific objective”. Thus, the ITIL-based “incident model” can be described as a procedure or a sub-process in the incident management process.

The expanded incident lifecycle (Office of Government Commerce 2011b, Office of Government Commerce 2011a) fits our purposes better than the previously mentioned concept of an ITIL incident model. It is defined in ITIL CSI and ITIL Service Design and describes the stages of the service lifecycle on a timeline. These stages are detection, diagnosis, repair, recovery and restoration. The expanded incident lifecycle is used to help understand all contributions to the impact of incidents and to plan for how these could be controlled or reduced. It also acts as a basis for the key performance indicators (KPI) and related metrics used in the availability management process (Fig. 18).
As mentioned in the beginning of this section, the incident model may be used in an incident investigation. One purpose of an incident investigation is to find the root cause of the incident. In addition to the incident model, we consider the root cause analysis (RCA) methods as a very useful way to collect evidence on how and why an incident or a problem occurred. Some of the RCA methods also open the background conditions, leading to the incidents. However, only two of them, 5-Whys and chronological analysis, provide an explanation of the factors leading to the incident.

Fault tree analysis (FTA) is presented in ITIL as a design tool (Office of Government Commerce 2011b). In other literature, it is considered an incident model or risk assessment tool model (Johnson 2003). All of these models can be categorized as linear/sequential models.

5-Whys RCA method works by starting out with a description of which events took place and then asking ‘Why did this occur?’ The resulting answer is given, followed by another round of ‘Why did this occur?’ Usually by the fifth iteration, a true root cause will be found.

5-Whys does not, however, give a framework, for where and how to look for these root causes. It is also a generic method with no adaptation to ITSM. It does not provide explanation, why to choose just the fifth root cause candidate, and omit the others. 5-Whys explains the incident as a result of a sequence of events, like
the domino theory. There is a fixed number, five “dominos,” without labels on them.

**Chronological analysis** is conducted by documenting all events in chronological order to provide a timeline of events. This often makes it possible to see which events may have been triggered by others – or to remove any claims of causes or conditions that are not supported by the sequence of events.

**Fault tree analysis (FTA)** is a technique that can be used to determine a chain of events that has caused an incident or may cause an incident in the future. In FTA, a representation of a chain of events is made using Boolean notation. As a very straightforward model, it can be configured in monitoring systems. Fig. 19 gives an example of a fault tree.

FTA is usually used as a technical model to design IT systems and to evaluate their availability. In the ITIL framework, FTA is used as a risk analysis tool in availability management (Office of Government Commerce 2011b, Office of Government Commerce 2011a). It can also be used as an incident investigation tool, which also takes into account all the possible events and conditions, including technical and human factors. Fault tree analysis extends the strict sequence of events by adding logical operators or logical gates (AND, OR) into the model (NASA Office of Safety and Mission Assurance 2002, Senel, Senel 2013, Xia et al. 2012).
The definition of incident is different in ITSM as opposed to other industries. These differences will subsequently be discussed. They also serve as one of the sources for the requirements for the IT incident model.

3.3 INCIDENTS IN IT AND IN OTHER INDUSTRIES

The nature of incidents in IT and IT service management is different from incidents in other industries. This may explain, at least partially, why existing established incident models are not used in the IT industry.

3.3.1 IT service incidents have a longer duration
Accidents have been broadly defined as “a short, sudden and unexpected event or occurrence that results in an unwanted and undesirable outcome” (Hollnagel 2004). The accident is over when the damage has occurred. In ITSM, this is only the beginning of the incident, as the incident is over when the service is restored. Thus, an IT service incident has a duration, which can last from seconds to weeks or months. During this period, the service user experiences a service downtime of reduced service quality. Thus, it is important to understand what happens before and during the incident, to mitigate the impact of it.

3.3.2 Fewer human errors in IT incidents
ITSM, however, has certain features, which makes the direct adaptation of incident models in the ICT domain more challenging than in other industries. In other industries, human errors cover 60-96% of the root causes of incidents, while in ITSM, the portion of human errors is only 18-25% (Table 2).

The high percentage of human errors in incidents in other industries affects the incident investigation and incident models. The human factors analysis and classification system (HFACS) is focused mainly on human factors. It is used in many industries as the primary tool in incident investigation.
Table 2. Proportion of human errors of root causes of incidents in different industries.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Human errors</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation</td>
<td>70-80%</td>
<td>(Wiegmann 2001)</td>
</tr>
<tr>
<td>Maritime</td>
<td>75-96%</td>
<td>(Hanzu-Pazara et al. 2008)</td>
</tr>
<tr>
<td>Railway</td>
<td>61%</td>
<td>(Aguirre et al. 2013)</td>
</tr>
<tr>
<td>Healthcare</td>
<td>70-80%</td>
<td>(Kohn, Corrigan &amp; Donaldson 2000, Hunziker et al. 2011)</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
<td>80%</td>
<td>(Cintron 2015)</td>
</tr>
<tr>
<td>Nuclear energy</td>
<td>80%</td>
<td>(International Atomic Energy Agency 2013, Ziedelis, Noel &amp; Strucic 2012)</td>
</tr>
<tr>
<td>Chemical industry</td>
<td>60-90%</td>
<td>(Raju 2014)</td>
</tr>
<tr>
<td>Telephony and Internet</td>
<td>19%</td>
<td>(Karsberg, Skouloudi 2015)</td>
</tr>
<tr>
<td>ITSM</td>
<td>18-24%</td>
<td>(Ponemon Institute Research Report 2013, Shwartz et al. 2010, Saarelainen, Jäntti 2015a, Marcus, Stern 2000, Quorum 2013)</td>
</tr>
</tbody>
</table>

3.3.3 The quality of IT incident reports is poor
In Papers III and IV, we observed that the quality of IT service incidents was poor. In Paper III, it was found that only 42% of the reports had enough information to be allocated in a HFACS category. In Paper IV, it was noticed that 27% had no root cause at all, and 27% identified more than one root cause or contributing factor.

According to our experience this is the situation all over in the ITSM industry: the reports tend to be brief. Reasons for this might include time pressure, the lack of resources in IT service provider organisations and the lower impact of average incident, as compared to other industries, where incidents may cause casualties.

The root cause analysis in the ICT industry is conducted at a fast pace, in hours or days, in contrast to, for example, aviation, where a major accident involving fatalities may take 6 months or more. In small aviation incidents, the report is prepared in 4-6 weeks (Aircraft Accident Investigation Bureau 2012).
Because of the low quality of the reports, it is challenging to conduct an incident trend analysis, since there is usually very little information on the root causes of the incidents. Hence, Paper III recommends categorisation of the incidents to be done already in an original investigation using the same model as in an incident trend analysis.

The quality of the reports depends on the competence and training of the investigators. The training for aviation accident investigators ranges from 5 day short courses to certificates covering over 30 training days (Southern California Safety Institute (SCSI)). An IT service incident investigator is often an ordinary subject matter expert, mostly without a formal root cause analysis training and even less human factor related training. This was observed during the interviews and discussions with the case organisation.
Kari Saarelainen:
How and why things happen - Anatomy of IT service incidents
4 Research phases and research methods

This section splits the research work into three phases and connects them to the research papers. The research methods are explained in general along with their application in this thesis. Data analysis principles are presented regarding all the papers in general and the specific methods and analysis applied in each.

4.1 RESEARCH PHASES

The research can be divided in three phases: 1) identification of the root cause categories, 2) conducting an incident investigation and trend analysis, and 3) establishing the IT service incident model. The phases of the research are presented in Fig. 20.

In Phase 1, Papers I and II focused on the categorisation of the incidents, which is a fundamental function in a trend analysis, especially when there is a large number of incidents. Paper I focused on the generic categorisation of incident root causes; Paper II focussed on human factors. Additionally, Paper I introduced a method to analyse categorized data effectively (multidimensional incident analysis).

Figure 20. The phases of the research.
In Phase 2, Paper III, it became clear that the same accident framework or model should be used in the original incident investigation and the trend analysis phase of the incidents. During the research, we observed that the HFACS, which is very popular in other industries, was not suitable for IT services as such (Paper III).

In Phase 3, Papers IV and V focused on developing the IT service incident model. This model goes far beyond categorisation. It also reaches the latent, contributing factors of the incidents and incorporates the root cause categories. This model could, and also should, be used in primary incident investigations and in an incident trend analysis. The capability of using conditional probabilities was added in the model in Paper V. This helps with planning the focus points in the upcoming incident analysis, risk analysis and service improvement efforts. Table 3 shows the research approaches that were used in the thesis. All the papers refer to the ITIL proactive problem management. Papers II–V are related to the incident models.

The research methods used in the papers are listed in Table 4. All of the papers are based on the same pool of incident reports, collected using the same case study methods. Action research was used in Paper I, when establishing these categories and evaluating the developed analysis method. Action research was also used in Paper III, when applying and evaluating the HFACS model on human error-related IT service incidents. The statistical significance of the results in Paper II were calculated using Fisher’s exact test. The IT Incident Model in Paper V was built using the design science research method in the Bayesian Belief Networks.

Table 3. Approaches used in the papers.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Reference</th>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITIL Proactive problem management</td>
<td>(Office of Government Commerce 2011)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Incident models</td>
<td>Several</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
The research question in this thesis “What tools, methods, practises and aspects should be included in the model for IT service incidents?” was further formulated in four additional research questions (RQ). These additional research questions and related papers are shown in Table 5. The root causes (RQ 1) are discussed in Papers I, II and III. RQ2 is addressed by introducing in The IT Incident Model (IIModel) (Paper IV) and Bayesian Belief Network as a tool in proactive problem management (Paper V). Events and conditions during an incident (RQ3) are discussed in Paper IV. The IT Incident Model (IIModel) and tools for proactive problem management (RQ4) are presented in Papers IV and V. Usage of the IIModel in incident investigation and in incident trend analysis (RQ4) is discussed in Paper III.

### Table 4. Research methods used in each paper.

<table>
<thead>
<tr>
<th>Method</th>
<th>Reference</th>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Paper I</td>
<td>Paper II</td>
<td>Paper III</td>
</tr>
<tr>
<td>Case study</td>
<td>(Yin 2003)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Within case analysis</td>
<td>(Eisenhardt 1989)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Action research</td>
<td>(Baskerville 1999)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fisher’s exact test</td>
<td>(Fisher 1954)</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Design Science</td>
<td>(Hevner, Chatterjee 2010)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bayesian Belief Network</td>
<td>(Gelman et al. 2013)</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

### Table 5. Additional research questions and related papers.

<table>
<thead>
<tr>
<th>Additional research question (RQ)</th>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Paper I</td>
<td>Paper II</td>
<td>Paper III</td>
</tr>
<tr>
<td>RQ1. How do incidents happen and how should the root causes of incidents be categorized?</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RQ2. Why do incidents happen and what events and conditions cause or increase the probability of an IT service incident?</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RQ3. What events or conditions during an IT service incident lengthen its duration or increase the impact of it?</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RQ4. How could the incidents in the ITSM operating environment be modelled to aid proactive problem management, root cause analysis and CSI?</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
4.2 **CASE STUDY METHOD AND DATA COLLECTION PROCEDURES**

According to Yin (Yin 2003), a case study is “an empirical inquiry that investigates a contemporary phenomenon within its real-life context”. The case study method in this thesis is applied to explore the deep structure, causes and contributing factors of incidents in the context of proactive problem management. The case study method was selected because it allowed for a rich data collection of unspecified, emerging and developing research domains by empirical means.

Multiple data collection methods proposed by Yin (Yin 2003) were applied during the study. The research data was gathered from the following data sources:

- **Documents**: Incident reports, process descriptions (change, incident, problem, event, capacity, configuration and release management processes, and human resource policies), work guides, and guidelines.
- **Interviews**: Experts, and customer services managers were interviewed regarding the incident cases, and process owners, process managers, various levels of managers, and human resource managers were interviewed regarding ITSM and organisational processes.
- **Participant observation**: Discussions with managers, supervisors and experts, observation of their daily ITSM work.
- **Records and archives**: Change, incident, and problem records.

The rationale for using multiple sources of data is the triangulation of evidence. Triangulation increases the reliability of the data and the process of gathering it. The incidents were reviewed with the report writer or the customer service manager. Where possible, the experts involved were also interviewed. Line supervisors and higher level management were also interviewed. Since the organisation was working in the matrix, the key process owners and process managers were interviewed. In the interviews of the line organisation, the training and experience of
the personnel were also examined, especially with those persons involved with the incidents. Organisational changes and training policies were also reviewed.

The objective was to study all the relevant incident reports available in the respective part of the research. Thus, no sampling of incident reports were conducted.

**Within case analysis** technique (Eisenhardt 1989) was used in the data collection phase. The incident categorisation scheme and findings were validated through discussions and improvement workshops with the representatives of the case study organisation. The principal author was responsible for producing a summary of the findings, which was delivered to the case organisation. The established incident categories were improved, taking into account the comments from the case organisation’s managers. Some new categories were added to the original classification.

The limitations of the case study method include a possible biased views of the researcher (Yin 2003). Systematic use of multiple data sources and confirmation and/or discussion of the conclusions with the interviewees mitigated the effect of researcher bias. Bias was also mitigated by using two researchers (researcher triangulation), where appropriate. Additionally, generalisation of the results does not aim to statistical generalisation, but to extend the theory of ITSM problem management and incident modelling by finding representative cases.

There are also limitations related to the collected data. First, the number of properly written incident reports was surprisingly low, resulting in a lower statistical credibility in some of the papers. Second, the reports were made by a certain IT service provider, which may not have provided a representative picture of the entire industry.

Although several different and independent environments were used, this did not cover the entire spectrum of IT environments. For example, there were no examples of cloud services or end-user support in the environments. Other
organisations, other clients, other environments, and other times may have given different results.

Yin (Yin 1998) recommends that researchers continually judge the quality of their case study design. There are four tests used to assess whether the study has met the requirements of construct validity, internal validity, external validity and reliability. According to Yin, these tests should be applied throughout the case study process: during design, data collection, data analysis and reporting. Table 6 summarises the recommended tactics covering these tests and shows the ways in which the research design and conduct for this case study followed these recommendations.

Table 6. Case study tactics and responses (Yin 1998).

<table>
<thead>
<tr>
<th>Tests</th>
<th>Case Study Tactic</th>
<th>Research phase in which tactic occurs</th>
<th>Action taken in this research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Construct validity</strong></td>
<td>Use multiple sources of evidence</td>
<td>Data collection</td>
<td>Use of incident reports, interviews, documents and physical artefacts</td>
</tr>
<tr>
<td></td>
<td>Establish chain of evidence</td>
<td>Data collection</td>
<td>The phases of selection and handling of material is documented and traceable. The chain between research question and data sources, findings and conclusions is documented.</td>
</tr>
<tr>
<td></td>
<td>Have key informants review draft case study report</td>
<td>Data collection</td>
<td>The root causes and their categorization were reviewed by report writers or related customer service managers.</td>
</tr>
<tr>
<td><strong>Internal validity</strong></td>
<td>Do pattern matching</td>
<td>Data analysis</td>
<td>Patterns i.e. incident root causes were identified across cases (Papers I and II)</td>
</tr>
<tr>
<td></td>
<td>Do explanation building</td>
<td>Data analysis</td>
<td>Causal links identified inside incidents (Paper IV)</td>
</tr>
<tr>
<td></td>
<td>Do time series analysis</td>
<td>Data analysis</td>
<td>Was performed as part of incident trend analysis.</td>
</tr>
<tr>
<td></td>
<td>Do logic models</td>
<td>Data analysis</td>
<td>Not performed.</td>
</tr>
<tr>
<td><strong>External validity</strong></td>
<td>Use rival theories within single cases</td>
<td>Data analysis</td>
<td>The thesis investigates rivalling causes and contributing factors to incidents. HFACS is applied as an initial theory.</td>
</tr>
<tr>
<td></td>
<td>Use replication logic in multiple-case studies</td>
<td>Data analysis</td>
<td>Multiple cases investigated using replication logic</td>
</tr>
<tr>
<td><strong>Reliability</strong></td>
<td>Use case study protocol</td>
<td>Data collection</td>
<td>Same data collection procedure followed for each case</td>
</tr>
<tr>
<td></td>
<td>Develop case study database</td>
<td>Data collection</td>
<td>Incidents were stored in a databases and the same or corrected incident reports were used in all the Papers.</td>
</tr>
</tbody>
</table>
4.3 RESEARCH WITH ACTION RESEARCH METHOD

The action research cycle by Baskerville (Baskerville 1999) was used in the research. Action research aims at an increased understanding of an immediate social situation, especially on the complex nature of this social setting in the IT domain. In this thesis, the social setting refers to IT service process dynamics with people, processes and tools. At the same time, action research focuses on practical problem solving and expands scientific knowledge. Practical problem solving increases the value of this thesis, because the new knowledge and results can be applied in the daily process improvement work by quality managers and process managers.

Action research is performed collaboratively. This is typical for process improvement initiatives. The participatory observation process is used to achieve this goal. Action research is primarily applicable for the understanding of change processes in social systems.

The action research cycle consists of five phases: A. Diagnosis, B. Action Planning, C. Action Taking, D. Evaluation, and E. Specifying Learning (Fig. 21).

There are certain limitations related to the action research method. First, action research typically includes several iterative research cycles. However, in Papers I and III, we focused on describing only one improvement cycle, due to the time constraints. Second, action research benefits from a collaborative effort. Although we used multiple data sources, more effort could have been put on collaborative actions, instead of a consultancy problem solving style.
4.4 **MODEL DESIGN WITH DESIGN SCIENCE METHOD**

The Design Science research method was selected for this study, since it provides a clear research process for constructing and validating models and methods. Hevner and Chatterjee (Hevner, Chatterjee 2010) propose, in scientific information systems, the design of a framework of three research cycles (Fig. 22): the Relevance Cycle, the Rigor Cycle and the Design Cycle.

The Relevance Cycle connects the contextual environment in the research project with the design science activities. The Rigor Cycle connects the design science activities with the knowledge base of scientific foundations, expertise and experience that feeds information to the research project. The Design Cycle, in the centre, iterates between building and evaluating the design artifacts and processes of the research (Fig. 22).

The questions in Table 7 provide a checklist, which has been used to assess the progress of design research projects (Hevner, Chatterjee 2010). The objective of the checklist is to ensure that the projects address the key aspects of the design science research. The numbers in Fig. 22 refer to the questions in Table 7.
**Figure 22. Three design science research cycles with design science research checklist questions mapped onto it.**

**Table 7. Design science check list.**

<table>
<thead>
<tr>
<th>Question</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What is the research question (design requirements)?</td>
</tr>
<tr>
<td>2</td>
<td>What is the artifact? How is the artifact represented?</td>
</tr>
<tr>
<td>3</td>
<td>What design process (search heuristics) will be used to build the artifact</td>
</tr>
<tr>
<td>4</td>
<td>How are the artifacts and the design processes grounded by the knowledge base? What, if any, theories support the artifact design and the design process?</td>
</tr>
<tr>
<td>5</td>
<td>What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle?</td>
</tr>
<tr>
<td>6</td>
<td>How is the artifact introduced into the application environment and how is it field tested? What metrics are used to demonstrate the artifact’s utility and improvement over previous artifacts?</td>
</tr>
<tr>
<td>7</td>
<td>What new knowledge is added to the knowledge base and in what form (e.g. peer-reviewed literature, meta-artifacts, new theory, new methods)?</td>
</tr>
<tr>
<td>8</td>
<td>Has the research question been satisfactorily addressed?</td>
</tr>
</tbody>
</table>
Hevner et al. (Hevner, Chatterjee 2010) provided seven guidelines that describe the characteristics of a design science research: 1) research must produce a viable artifact created to address a problem, 2) the artifact should be relevant to the solution of a business problem, 3) the utility, quality, and efficacy must be rigorously evaluated via well executed evaluation methods, 4) the research must provide a verifiable contribution, 5) rigorous methods must be applied in the design and evaluation of the artifact, 6) available knowledge and theories are used in the development of the artifact, and 7) the artifact is effectively communicated to appropriate audiences. As such, no detailed process for performing design science research is proposed. The checklist in Table 7 has been used to assess progress on design research projects, including the previously presented guidelines.

4.5 ANALYSIS

4.5.1 Data analysis related to all papers
The same pool of incident reports were used as a basis for the data analysis in all of the Papers. The selected set of reports was used depended on the focus in each paper. The data were collected in years 2012 – 2014 at a large IT service provider on several distinct occasions, which reflected several customers and several types of separate and shared environments. The incident reports were separate reports, including a root cause analysis, provided that the root cause was found. In the ITIL framework, these incident reports could be characterized as major problem review reports. All of these service environments were maintained by a single IT service provider. Environments consisted of several types of systems dedicated to the client, in the premises of both the client and the service provider. Some of the environments were also shared with several customers.

The total number of incident reports was 212. Deviation of some reports in the results is possible, since some duplicate reports were found during the study. In some studies, there were several distinct causal chains in the same report (e.g. one leading
to the incident and another leading to another incident within the incident). For practical reasons, these were considered in Papers III, IV and V as separate incidents. Since the research was conducted during different periods of time, not all incident reports were available, when the individual papers were developed.

4.5.2 Analysis in individual papers

**Paper I:** In Paper I, the analysis was based on 174 incident reports. The root causes were categorized. Within case method was used to refine the set of incident categories and root cause categories. The incident categorisation scheme and findings were validated through discussions and improvement workshops with the representatives of the case organisation. A summary of the findings was delivered to case organisation’s representatives. The established incident categories were improved, taking into account the comments from the case organisation’s managers. Some new categories were added to the original classification.

**Paper II:** In this paper, 62 incident reports related to human errors were analysed and categorised by the HFACS categories. The hypothesis of HFACS is that the incident happens, when successive organisation levels (slices of Swiss cheese) fail (hole in the slices). In this research, the failures in the different HFACS root cause categories were inspected. The results were validated statically with Fisher’s exact test. After this, the incident categories and root cause categories were analysed with the multidimensional incident analysis method (MIA), introduced in Paper I. The analysed dimensions were derived from the HFACS and ITIL processes.

**Paper III:** The analysis focused on 72 human error-related incidents captured from IT service organisation’s service managers and the documentation and ITSM tools. As supplementary and reference materials, there were an additional 51 incident reports with human error contributions from the same
IT service organisation’s other environments. The planned action phases in this study were:

1. Analysis of the incident reports: The action planning phase started by analysing the human error related incident reports, interviewing related persons and reviewing relevant facts from other sources. The root causes of the incidents were reviewed against the HFACS framework and its root cause categories. The root causes classified by the HFACS categories were analysed.

2. Analysis of incident investigation processes: The incident investigation process was studied as part of the CSI. The primary incident investigation process was compared to the post incident investigation based on the existing incident reports.

**Paper IV:** 215 incidents and their root causes, contributing events and conditions, were studied. Their sequences were extracted from the reports. In those reports, the direct root cause was clearly stated, if it was found. The other events and conditions were extracted from the narrative report text and other data sources described previously. All 15 incident reports with three or more root causes or contributing conditions were chosen for the validation of the IT service incident model.

**Paper V:** In this paper, all 67 incidents where two or more root causes could be identified either in the report, interviews or other data sources were analysed. The data analysis consisted of the following steps:

1. Identification: The root causes were identified from the incident cases by incident reports, interviews of relevant people and from log and ticket information. If there were several root causes, the chains of events and causal links between the root causes were identified and documented.

2. Categorisation: The root causes were categorized in detailed categories according to the IT service incident framework.
3. Creating a Bayesian Belief Network (BBN): The data was fed into a BBN tool, which constructed the BBN and calculated the conditional probabilities. The BBN network can be seen as a logical model that is one of the case study analysis techniques proposed by Yin (Yin 2003).

4.6 EXPERIENCES GAINED

The different phases of data collection were conducted very fluently. The data collection and part of the analysis were organised as several separate projects sponsored by the case organisation. The projects were recognised service improvement efforts and had strong management support in the case organisation. Because of this, all the resources were accessible and the researchers were able to carry out the projects in a timely manner. This experience underlines management’s role in service improvement efforts in a similar way to how the management contributes to IT service incidents in the IT incident model discussed later in this thesis.

Some of the projects were conducted together with the clients of the case organisation. In these projects, the case organisation and the client worked together in a common service improvement project. All the results, findings and planned improvement actions were disclosed openly to all the parties. During those projects, this resulted in a tangible improvement in the client relationship. This effect was so strong that this kind of mutual service improvement effort could be considered as one kind of business relationship management. This side of the project was, however, out of the scope of this research and is not discussed further in this thesis.
5 How incidents happen – Incident root cause categories

One of the key tasks in proactive problem management is incident trend analysis. This is promoted by several ITSM frameworks (e.g. ITILv3, ISO 20000 and COBIT5) (Office of Government Commerce 2011c, ISO/IEC JTC 1, SC 7 2011, ISACA 2012). According to ITIL, trend analysis is “analysis of data to identify time-related patterns”. In this chapter, we propose that the scope of the incident trend analysis should be extended to a more sophisticated analytics.

Including the root causes in the analysis and combining it with other pieces of information greatly enhances the power of analytics, as compared to the traditional approach. Including root causes in a trend analysis requires the categorisation of root causes according to the same taxonomy. In this chapter, we will discuss these taxonomies. Special attention is paid to human factors and incidents, including their latent, contributing factors.

5.1 MULTIDIMENSIONAL ANALYTICS OF INCIDENTS

Incidents and problems must be logged after identification. Thus, they form a collection of log files. All methods and tools used to deal with log files, in general, are can be used also with incident and problem logs. The incident and problem records typically answer the questions of when (the incident happened), what (CI was affected), who (was involved) and why (did the incident occur, i.e. what was the root cause) (Office of Government Commerce 2011c).
5.1.1 Categories of root causes of IT service incidents
An analysis of a large number of incidents may reveal the same patterns across a number of cases leading to common contributing factors. The challenge in including root causes in an incident trend analysis is that details of diagnostics and root causes are usually descriptive text, which are difficult for analysis tools to handle. To statistically analyse a large number of root causes in incident and problem records, one has to map the varying terminology from different records into a uniform, normalized terminology. In Paper I, a multidimensional analytics approach, including the categorisation of incidents and their root causes, is proposed.

By definition, “IT service is made up of a combination of IT, people and processes.” This is a natural and the most common approach for the upper level categorisation of root causes of IT service incidents. This is also the basic categorisation principle that is supported by most of the accident models from various industries, as is observed in Paper IV.

Paper I studies incident categorisation via a case study. In this case, technology was decided to further divide the root cause categories related to incidents caused by software, firmware and hardware. The data to support categorisation decisions was derived from multiple sources using case study data collection methods. In the production environment, the most effective way to categorize the incident root cause is already in the incident investigation phase, using the same model as in an incident trend analysis, as proposed in Paper III. In Paper I, we also recommended the categorisation of responsible parties to get a clear picture of who was involved with the incident.

5.1.2 Towards more sophisticated incident analytics
Analytics means discovery, interpretation, and communication of meaningful patterns in the data. Analytics is widely used in a variety of business operations, including business analytics, marketing, risk analytics, security and IT system log analytics. Paper I proposes an analytics-based incident analysis method called the Multidimensional Incident Analysis Method (MIA). In
this method, two dimensions at a time are analysed simultaneously in a matrix. The colour coding of cells helps to visualize the results. The analysed dimensions can be any of the fields stored in the incident or problem records or derived from them. The only requirement is that these fields have to be discrete to enable the calculation of how many incidents are related to them. Continuous fields (e.g. time) have to be split into discrete blocks (e.g. months, weeks or days).

An example of MIA in incident analysis is shown in Fig. 23, where the analysed dimensions are the root cause and incident categories. In this example, the number of errors in the incident category “network” is 33% of all the errors. This is also the result of a traditional incident analysis by incident type. By adding the root cause category as another dimension, it is apparent that human errors (10.3%) related to a network are a major improvement area in IT service quality.

Additionally, software errors in applications (8.5%) and servers (6.7%), as well as hardware errors, should be inspected. In a similar way, the dimensions may be an arbitrary combination of the incident type, root causes, time, responsible party or location.

![Figure 23. Example of incident category - root cause category analysis (Paper I).](image)
5.1.3 Incident trend analysis and incident investigation
There is no universal process for an incident investigation. In Paper III, we observed that the identified incident investigation processes share common features. The analysed processes (ESReDA Working Group on Accident Investigation 2009, Bureau of Land Management 2003, Risktec 2008) contain data collection, analysis and findings/reporting phases. Some of the process descriptions also contained the planning phase in the beginning, or corrective actions phase in the end, of the accident investigation.

The approach used in this thesis is the process of European Safety Reliability and Data Association (ESReDA) (Fig. 24). ESReDA splits an incident investigation into five phases: I. Collecting data, II hypothesis generation, III analysis, IV findings and V recommendations. Phases I, II, III and IV together are often called the root cause analysis (RCA).

An incident trend analysis aims to study the historical incident records. Using any incident model, taxonomy, categorisation or classification in an analysis of historical incident records isolated from the original incident investigation process has certain drawbacks (Fig. 25).

![Diagram of ESReDA process]

*Figure 24. Original, primary incident investigation using ESReDA process.*
How incidents happen – Incident root cause categories

The first drawback is that the incident trend analyst does not usually have the same “initial, a priori information, model A” that was used in a primary incident investigation. In the case of IT service incidents, no incident model is commonly used in the primary investigation. Reliable categorisation of root causes is difficult, because of the different categorisation principles related to different incident models in a primary investigation and analysis of historical records.

The second drawback is that the iterative part of the process in a primary incident investigation (Fig. 24) is missing in the post incident investigation (Fig. 25), which causes difficulties in categorisation. For example, suppose that the root cause in the report is a “configuration error”. Did this occur because the employee did not know how to configure the device or made a typo? Was the error based on false information of environment or configuration parameters? Was testing routinely or exceptionally skipped, where the bug would have been discovered before the transfer to production? Revising and refining the root cause or testing a new hypothesis is difficult without the possibility of collecting more data, when new questions or hypothesis arise.

The third drawback is that the quality of IT service incident records is poor and the information provided is very brief. An incident trend analysis of incident reports when the same model,
framework or categorisation principle is not applied in the original, primary incident investigation is common practice in other industries (Ergai 2013). This is understandable, since, for example, an aviation accident report is prepared over the course of 4 weeks to 6 six months, depending on the severity of the accident (DOE 1999, Aircraft Accident Investigation Bureau 2012). The publicly available aviation reports of the National Transportation Safety Board (NTSB) are very extensive and typically cover from 60 to over 100 pages of written material.

Reports or records of IT service incidents are prepared in minutes, hours or days. These reports consist of some explanatory words, lines or pages, in the case of major incidents. It is possible to conduct an analysis from different viewpoints from an exhaustive report, where the most of the essential information is collected. A very compact IT incident report often lacks the essential related information and may contain only the conclusion (“configuration error”).

These challenges lead us to a conclusion: to obtain more accurate results, an incident categorisation model or any other incident model should be taken into account in the data collection phase of the original incident report. The categorisation of the root causes should be conducted in the investigation phase, when there is the possibility of testing different hypotheses. This is even more important when using more complicated incident models, e.g. HFACS or the IT Incident Model (IIModel), which will be presented later. These models can guide the incident investigation from apparent, direct causes to explore the contributing factors of the incidents. Another reason for using the incident model and performing categorisation in incident investigation is the partial automation of a proactive problem management process. If the root cause categories were stored in incident/problem records, one could build, for example, a real-time dashboard of incident situations instead of a manually performed trend analysis exercise once or twice a year.
6 Why incidents happen – The IT Incident Model

In this section, we construct the incident model related to the root causes and the extended model of the incident lifecycle. Requirements of the incident model are developed based on studies on existing incident models and on the information about the special nature of IT incidents. A hierarchical taxonomy and a graphical time presentation are presented. This model is then adapted to a Bayes network of conditional probabilities with a set of real-life incidents and their relationships and probabilities. Finally, the different parts of the model are presented in a framework of proactive problem management and incident investigation processes.

6.1 REQUIREMENTS FOR AN IT INCIDENT MODEL (IIMODEL)

This section addresses additional research question 4: How can the incidents in the ITSM operating environment be modelled to aid proactive problem management, root cause analysis and CSI? Paper III shows that one the most popular incident models, HFACS, is not suitable for investigating IT service incidents. The nature of an incident is different than that of other industries, as described in Section 3.1.2.

To choose or develop an incident model suitable for use in ITSM, a requirement list was created. The following requirements for the model were derived from the research papers of this thesis or they were identified as necessary or useful features in other
incident models. This model is called the IT Incident Model (IIModel).

**Compatibility with ITIL:** The model should be compatible with ITIL and with the proactive problem management process introduced in Section 3.1.1 and presented in Fig. 26. These both form the core frameworks of this thesis.

**Compatibility with the root cause definition:** Paper II presents the following definition to the root cause: “Root causes are the underlying causes of an incident or a problem, which if corrected would prevent or significantly reduce the likelihood of the incident’s reoccurrence.” The model should be compatible with this definition. This means that the model has to allow for several root causes. Additionally, a recommended feature is to describe or handle probabilities or likelihoods, as mentioned in the definition.

**Usage as a primary and secondary tool:** Paper III recommends using the same tool in the original investigation (primary tool) and incident trend analysis, based on historical incident records (secondary tool). The model should be useful in both of these roles.

**Simplicity, low training requirement:** The training of accident investigators ranges from 5 day short courses to certificates covering over 30 training days (Southern California Safety Institute (SCSI)). In the IT domain, the incident investigator is often an ordinary subject matter expert mostly without formal root cause analysis training and even less incident investigation related training. The training should be possible to be given to novice incident investigators in a matter of hours, instead of days or weeks.

---

**Figure 26. Proactive problem management cycle.**
Low resource requirement in analysis: The root cause analysis in the ICT industry is done at a fast pace (i.e., hours or days), in contrast to aviation, where a major accident involving fatalities may take 6 months or more. In small aviation incidents, the report is prepared in 4-6 weeks (DOE 1999, ISACA 2012). The model should add as little overhead to the incident investigation as possible.

Taxonomy: Incident trend analysis is an essential part of proactive problem management. Analysing simultaneously large numbers of incident root causes, as in an incident trend analysis, requires the classification of root causes according to a generic or organisation specific taxonomy (Salmon, Cornelissen & Trotter 2012). Additionally, taxonomy guides the incident investigator in data collection and increases the reliability of investigation results (Salmon, Cornelissen & Trotter 2012, Underwood, Waterson 2014). One of the most popular incident models, the HFACS, is basically a hierarchical taxonomy.

The taxonomy should cover all the available known root causes. At the minimum, the basic building blocks of IT services, people, technology and processes (Office of Government Commerce 2011c), should be there. Additionally, the causes coming outside of the direct control of an ITSM organisation, “external factors,” such as forces of nature and cyber-crimes for investigating IT service incidents, should be addressed.

The same building blocks are present in other frameworks. Already the early and well known Leavitt’s model of organisational change presents that every organizational system is made up of four main components: people, task, technology and structure (Leavitt 1965). Dahlberg, Hokkanen and Newman have proposed that structure could be interpreted as strategy, business model and governance to reflect better the current roles and tasks of CIO (Dahlberg, Hokkanen, Newman 2016).

Graphical presentation: A graphical description of the incident helps communication among the investigators, the interviewees and the stakeholders. It makes it easy to identify information gaps (Sklet 2004, Svedung, Rasmussen 2002). The graphical representation of an incident has been considered to be
useful by both researchers and practitioners (Underwood, Waterson 2014).

**Hierarchy of root causes, events, conditions and contributing factors:** The analysis of the IT incident reports in Paper IV suggest that one incident may consist of several chains of causes, events and conditions before and during the incident. Thus, the capability to present this is also required from the model.

**Time presentation:** Unlike the incidents in most of the other industries, IT service incidents have a duration, which may be very long. The lifecycle of an incident is presented in ITIL as a timeline (Office of Government Commerce 2011b, Office of Government Commerce 2011a). The model should be able to present the events and other causal factors on a timeline. The objective is that the presentation in the incident model could be seen as an extended presentation of the incident lifecycle. Additionally, Paper IV introduces the concept of the “incident within the incident”, which is common in IT service incidents. A description of this requires the presentation of events and conditions in a timeline.

### 6.2 CONSTRUCTION OF THE IIMODEL

Our research indicate that instead of direct root causes, one should focus on the latent, underlying factors and conditions behind the root causes (Papers II, III and IV). Most of the current mainstream models describe and even name the possible sociotechnical layers: In Reason’s Swiss Cheese Model, the layers are the most fundamental part of the model (Reason 1990). HFACS has four layers (Shappell, Wiegmann 2001). Accimap by Rasmussen has six named layers (Rasmussen et al. 2010), while STAMP reuses Rasmussen’s layers (Leveson 2004). MTO has an undefined number of layers and failed barriers (Rollenhagen 1995). Even the domino theory has defined organisational factors, where the failures in sequence lead to the accident and injury.

HFACS is a very common incident model and one of a few models with a taxonomy. Thus, it was the starting point of the
IIModel construction. HFACS, as such, was soon found to be unsuitable for IT purposes. It was observed in Paper III that the HFACS taxonomy bears the heritage of the aviation context, and should be at least partially changed to comply with the IT context.

HFACS, with its 19 categories, is complicated, and thus, contradicts the simplicity requirement. The most serious deficiency is that the HFACS deals only with human errors. In the other industries, the amount of human errors is 60-96%; in IT services, it is 18-24%, as presented in Paper IV.

To keep the model as simple as possible, the number of layers should be as small as possible. The minimum number of layers is three, which was the amount of layers adopted in the model. Behind the direct causes to incidents are the inadequate conditions. These are, in turn, caused by organisational factors, management, and processes.

6.2.1 The taxonomy
HFACS taxonomy was used as basis for the categories of human errors, but as a simpler version: categories in human errors were cut to six from the original nineteen categories of the HFACS. Categories in technical conditions are influenced by the study of Marcus and Stern (e.g., forces of nature, cyber-crime) and our own statistics of incident reports. Franke has validated these categories through interviews with 50 availability experts (Franke et al. 2012). Hinz and Gewald (Hinz, Gewald 2006) have studied latent factors contributing to IT infrastructure risks with a desktop focus using expert interviews. These higher level risk categories can be used also as general categories of technical contributing conditions. Direct technical causes are taken from Paper I.

This taxonomy is not the definitive final taxonomy, since, in different environments, different root cause categories are dominant. There is a category “other” in each level, as proposed by Paper I. This taxonomy may be used as is or it can be adapted to local conditions. Guidelines for the local taxonomy or categorisation generation are described in Paper I. The taxonomy is shown in Fig. 27; it is discussed in more detail in Paper IV.
6.2.2 Presentation of incident scenarios

According to the requirements, the model should have graphical presentation capable of presenting events and conditions in a time sequence, describing a different hierarchy of root causes and contributing factors. From the accident investigation methods described in Section 2, Accimap, HFACS, STAMP and FRAM do not present time sequences. The Domino model, events and causal factors chart (ECFC) and the MTO have a timeline presentation and ability to model the hierarchical layers of causality. The MTO uses the ECFC presentation directly as part of its incident diagram. The Domino model is considered outdated as an incident model, and therefore, was not considered as an option.

Since the ECFC is well established and is a common presentation format, it is a natural choice as the basis for the presentation of incident scenarios. There are different versions of the ECFC presentation with different symbols for events, conditions, root causes and incidents, depending on whether they are presumed or based on actual evidence. These are connected...
The things may be colour coded to reflect the class of the cause in the taxonomy. This presentation forms a directed graph, making it directly compatible with a Bayesian Belief Network (BBN) presentation. This simplified variation of ECFC is called here the Simple ECFC (SECFC). The graphical presentation of the incident scenarios were introduced in Paper IV is shown in Fig. 28.

Figure 28. SECFC presentation of causality and time in an extended incident life cycle. The layers and colours are the same as in Fig. 27.
6.2.3 Presentation of probabilities
A graphical representation of the events and conditions are presented in Section 6.2.2 as a directed graph, which can always be presented as a Bayesian Belief Network (BBN). In the BBN model, one may add the probabilities of events (parameters in BBN). Thus, it can be used as a predictive tool (e.g. in risk assessment or to aid in the hypothesis generation and analysis phases). Usage of the BBN in the model is presented in Paper V.

6.3 THE IIMODEL AND MIA IN THE PROACTIVE PROBLEM MANAGEMENT FRAMEWORK

The major artifacts of this thesis are the IT Incident Model (IIModel) and Multidimensional Incident Analytics (MIA) method.

The IIModel consists of three tools, which are related to each other: the taxonomy of the categories of causal factors, the simple events and causal factors chart (SECFC) and the BBN analysis tool. The taxonomy and SECFC can be used throughout the incident investigations process.

BBN is mainly used in the risk assessment phase, where the following cycle of proactive problem management is planned. The results of the previous proactive problem management cycle (new statistical data, new relationships of causal factors) are also fed into the BBN model. The BBN may also be used in the incident investigation phase II Hypothesis generation to generate and test the different hypotheses. The relationship of the different parts of the incident model and proactive problem management cycle is shown in Fig. 29.
Figure 29. The components of the IT Incident Model (IIModel) and their use in different phases of the proactive problem management process.

The Multidimensional Incident Analysis (MIA) method, introduced in Paper I, is also presented in Fig. 23. MIA is an incident trend analysis method, where the various dimensions of a large number of incidents are analysed simultaneously. One of these dimensions is the direct root cause of the incidents, according to the direct cause layer in the taxonomy. It is recommended that the data be collected (Phase I Collecting data) in a form, where it can be directly used in the latter phases. MIA is a useful method to point to potential conditions (Phase II Hypothesis generation) or to analyse a given hypothesis (Phase III Analysis).
7 Summary of the papers

This section summarizes and reviews the original papers, illustrates their relationships and presents their contributions. The papers and their relationships are shown in Fig. 30.

Figure 30. The papers and their relationships with each other.

7.1 RELATIONSHIP OF THE RESEARCH PAPERS AND IT SERVICE MANAGEMENT

The research papers are related to proactive problem management. Proactive problem management is one form of ITIL CSI. The fundamental tenet in CSI is the Plan-Do-Check-Act cycle (Deming cycle), which describes the quality improvement process. The seven-step improvement process presented in CSI can be viewed as an example of an implementation of the PDCA cycle, with each of the steps falling within one of the phases of the cycle: Plan, Do, Check, Act.

An example of proactive problem management activities includes conducting periodically scheduled reviews of incident
records to find patterns and trends in the reported symptoms that may indicate the presence of the underlying errors in the infrastructure. Major problem reviews can also be a source of input to proactive problem management through the identification of underlying causes that may be discovered in the course of the review.

In Paper III, an accident investigation process by the European Safety Reliability and Data Association (ESReDA) (ESReDA Working Group on Accident Investigation 2009) was used as an example of a process, which could be used in proactive problem management. The investigation process is suitable to an incident trend analysis and an analysis of a single incident.

Fig. 17 summarises the PDCA cycle, seven step improvement process and incident analysis, using the accident analysis process by ESReDA. Fig. 31 includes the research papers, which have contributed to these phases of the accident investigation and proactive problem management. Table 8 presents a detailed list of the contributions of the research papers and their corresponding phases.

![Figure 31. Contributions of research papers located in the PDCA cycle, ITIL seven step improvement process and the ESReDA accident investigation process.](image-url)

Kari Saarelainen: 
How and why things happen - Anatomy of IT service incidents
Table 8. Research papers and their detailed contributions to the PDCA cycle, seven-step improvement process and the ESReDA accident investigation process. The colours are as in Fig. 31.

<table>
<thead>
<tr>
<th>PDCA: Stage of the cycle</th>
<th>PLAN</th>
<th>DO</th>
<th>CHECK</th>
<th>ACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITIL CSI: Step in the seven step improvement process</td>
<td>1. Identify the strategy for improvement</td>
<td>3. Gather the data</td>
<td>5. Analyse the information and data</td>
<td>7. Implement improvement</td>
</tr>
<tr>
<td>ITIL proactive problem management</td>
<td>Initial, a priori knowledge, model</td>
<td>Phase I: Data collection</td>
<td>Phase III: Analysis of the mixed incident and incident root cause categories</td>
<td>Implement recommendation(s)</td>
</tr>
<tr>
<td>Title of the publication ↓</td>
<td>Incident and incident root cause categories</td>
<td>Phase II: Hypothesis generation</td>
<td>Presentation of HE categories</td>
<td></td>
</tr>
<tr>
<td>I Creating an ITIL-based Multidimensional Incident Analytics Method: A Case Study</td>
<td>Analysis and presentation of the mixed incident and incident root cause categories</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>II Quality and Human Errors in IT Service Infrastructures</td>
<td>Analysis of human errors (HE)</td>
<td>Presentation of HE categories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III A Case Study on Improvement of Incident Investigation Process</td>
<td>Principle of using the incident model already in the original accident investigation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IV The Anatomy of IT Service Incidents</td>
<td>Causal chains of gathered data</td>
<td>Identify the causal chains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>V A model for analysing of information systems incidents: proactive approach</td>
<td>Taxonomy of the model</td>
<td>Structure of the model</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BBN analysis of causal chains</td>
<td>Identifying the causal chains</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graphical presentation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.2 SUMMARY OF PAPERS

For each article, the author of this thesis was the corresponding author with the most contributions. All of the data used in the research papers were gathered by the author. In all of the papers, the co-author, Marko Jäntti, reviewed the paper, provided valuable comments and helped with the introduction, scientific methods and literature. Regarding Paper V, the third co-author, Mika Hujo, helped with the theory and the tools of the Bayesian belief networks (BBN) and also reviewed the results. The following sections briefly describe the research papers.

7.2.1 Creating an ITIL-based Multidimensional Incident Analytics Method: A case study

The main contribution of Paper I was to introduce a new analytics method, multidimensional incident analysis (MIA), for an incident trend analysis. In this method, the incidents are categorized by the incident type and by the root cause type. The results are presented in a table format, where the incident type
and the root cause type are the dimensions. Other dimensions (e.g., time, ITIL process or responsible party) can be added easily.

The method also contains the process for categorising other dimensions, such as the responsible party. With this method, it is easy to locate the human errors in certain groups, or hardware, or software errors in a certain type of configurable item. The method includes processes for how to choose categories for incidents and other dimensions. The method was validated by applying it to an incident trend analysis in the case study organisation.

The research followed the action research cycle proposed by Baskerville (Baskerville 1999). Data was collected using the case study techniques (Yin 2003). It was analysed within the case analysis technique (Eisenhardt 1989). The publication was presented at the Tenth International Conference on Systems ICONS, where it was granted the best paper award.

7.2.2 Quality and Human Errors in IT Service Infrastructures - Human Error Based Root Causes of Incidents and Their Categorisation

The main contribution of Paper II was to apply the multilevel taxonomy of the root causes of incidents related to human factors in ITSM incidents.

The research problem of this study was how the quality of service could be improved by an analysis of incidents with root causes related to human errors. Our approach was to use the same taxonomy in the root cause categorisation as is used in accident investigation. The Human Factors Analysis and Classification System (HFACS) is a model and taxonomy. HFACS is commonly used with industry specific adaptations on various industries.

The total pool of incident reports related to human errors was 62 reports. Only 18 incident reports in this pool contained enough information to track the contributing conditions behind the harmful human act. These conditions were investigated using HFACS. As a result, three major types of sequences of events and
causal chains were identified. These event sequences describe the error pathways leading to the active failure.

By using a multidimensional incident analytics (MIA), two categorisation models, HFACS and ITSM processes, were analysed in a two dimensional matrix. Our findings showed that most of the error pathways were related to change planning.

Additionally, it was found that HFACS taxonomy is at least partially not compatible with ITSM concepts. Some HFACS categories were likely to cause confusion. An IT adaptation of the HFACS taxonomy could be part of our future work. HFACS itself models human factor related incidents with human factor related latent conditions, and omits everything else. In real life, the incident is contributed by technical, environmental, legislative, commercial, financial, weather conditions, and other factors, in random order. Ideally, one should be able to integrate all of these into the same model, which could explain and even predict the incidents.

The material was collected using case study methods (Yin 2003). The statistical significance was verified using Fisher’s exact test (Fisher 1954). Data was analysed using the multidimensional incident analytics (MIA) presented in Paper I.

7.2.3 A Case Study on the Improvement of the Incident Investigation Process

The main contribution of Paper III was the conclusion that an IT incident framework or model should be present already in the original, primary incident investigation phase. Applying incident models or advanced taxonomies to files, reports or logs, which are compiled without this knowledge about incidents, may lead to poor results.

The research problem in this study was: How can human errors, as root causes, be processed as part of service improvement efforts? In the case study, we applied a Human Factors Analysis and Classification System (HFACS) analysing 70 IT service related incidents.

Based on the analysis, several improvement suggestions were identified in ITSM processes of case organisations, including the
need for a taxonomy or an incident model adapted to ITSM (ITSM), improvements in the incident investigation process and coupling the incident investigation to the CSI. Improvement suggestions related to the HFACS model were also identified.

The research was conducted according to the phases of the action research cycle. Multiple data collection methods proposed by Yin were used during the study.

7.2.4 The Anatomy of IT Service Incidents

The main contribution of Paper IV was an incident model, which is adapted to the ITSM environment.

The research problem in this study was: How can the incidents in the ITSM operating environment be modelled to aid in proactive problem management, root cause analysis and CSI. The HFACS model was studied in Papers 2 and 3. The usability of the HFACS model for ITSM was analysed.

In this study, we identified some shortcomings of the HFACS, in general, and which applied to ITSM. These shortcomings are as follows: 1) HFACS is a complex system. 2) HFACS taxonomy has its roots in aviation, which is partially unsuitable to ITSM. 3) HFACS only covers human factors, while IT services are, by definition, made of a combination of people, technologies and processes. And 4) IT service incidents may have a longer duration, as compared to incidents in other industries.

The model designed during the study had a simple structure. It includes technology factors, process influence, and human factors. It has a time based presentation form. The model is validated by using 15 incident cases. Case study methods proposed by Yin were used in the data collection process.

7.2.5 A model for analysing information systems incidents: A proactive approach

The main contribution of Paper V was to enhance the IT Incident Model presented in Paper IV by using the Bayesian belief networks.

The research question was: How can the incidents in the ITSM operating environment be modelled to aid in proactive problem
management, root cause analysis and CSI? A combination of broadly accepted frameworks, ITIL incident frameworks, and a Human Factor Analysis and Classification System (HFACS) were used as basis for the new model. HFACS was extended to include human, technical, and external factors, and organisational processes.

The results of the analysis were entered in a Bayes belief network (BBN). Design science was used as a research method to design the incident model method. The model was validated using 67 incidents. The BBN was populated by the occurrences of different root cases, events and conditions.

The model calculates a probability network of root causes, events, and conditions, based on real incidents. Compared to earlier incident models, our model is designed for an ITSM environment, recognises several types of latent contributing factors to IT service incidents and accepts the large number chains of events leading up to an incident. The model can be used in proactive problem management, CSI of IT services, in what-if-analysis, and also as a tool in root cause analysis.

The model was designed using the Design Science Research method. This involved identifying and defining the requirements for an incident model in an IT service environment.
Kari Saarelainen:
How and why things happen - Anatomy of IT service incidents
8 Conclusions

Availability and continuous operation of IT services are essential to virtually all the functions of a modern society. However, there are very few studies regarding how and why unplanned IT service interruptions and incidents emerge and what are their contributing conditions. The research problem of this thesis is the lack of models or frameworks for managing IT service incidents. The short-term goal of this study is to develop an IT Incident Model with practical tools and methods. The long-term goal is to extend knowledge and understanding of incidents and their contributing factors. Several different incident models from other industries contributed the development of the IT Incident Model. Additionally, a cyclic proactive problem management model was created, and the elements of the IT Incident Model were placed within it.

The data was collected from over 200 incidents using the case study method (multiple data collection and triangulation) and the action research method. The IT Incident Model was created using the Design Science research method.

8.1 CONTRIBUTIONS OF THE THESIS

This research contributes to the ITSM research, particularly in the incident investigation and root cause analysis, by extending the ESReDA accident investigations process to comply with the seven-step improvement process and the PDCA cycle of the ITIL. This thesis presents a cyclic proactive problem management process that can be used by problem managers, CSI managers and quality managers to improve the quality of IT services.

For an incident trend analysis, we proposed an initial categorisation of the root causes of IT service incidents and
principles to adapt this to the IT service environment. These root cause categories can be used as one dimension when applying the incident analytics method (Multidimensional Incident Analytics, MIA), which was created during this research. The MIA helps in an incident trend analysis to locate the areas which may produce reoccurring incidents. Multidimensional analytics expands the scope of the incident trend analysis from the “analysis of data to identify time-related patterns”, as in the ITIL definition to more sophisticated analytics.

An important observation was the difference between incidents in the IT service industry and in other industries. There were several differences regarding incident duration, proportion of human factor related root causes, time used in the incident investigation and the quality of the incident reports. These differences lead to a recommendation to use the same incident model, both in the original incident investigation and in the incident trend analysis.

There is an overwhelming amount of incident models with a background in safety and accident prevention and analysis. However, none of these seem to adequately address the requirements of the ITSM, ITIL and proactive problem management. Therefore, a new model for IT incidents (IT Incident Model, IIModel) was created. IIModel consists of three major parts: 1) Hierarchical taxonomy of causal factors in IT service incidents, 2) A Simple Events and Causal Factors Chart (SECFC) and 3) The Bayesian Belief Network (BBN) analysis of the incidents.

8.2 DISCUSSION

8.2.1 Research questions
The research question aimed to determine what tools, methods, practises and aspects should be included in the model for IT service incidents. It was further divided in the following additional research questions: RQ1: How do incidents happen and how should the root causes of incidents be categorized? RQ2:
Why do incidents happen and what events or conditions cause or increase the probability of an IT service incident? RQ3: What events or conditions during the incident lengthen its duration or increase the impact of it? RQ4: How could the incidents in the ITSM operating environment be modelled to aid in proactive problem management, root cause analysis and CSI?

Regarding the first research question (How do incidents happen and how should the root causes of incidents be categorized?) direct root causes and their categories are in focus. We analysed root causes with other parameters (Paper I), mapped human error related root causes to ITIL processes (Paper II) and studied the distribution of human error related root causes (Paper III).

Concerning the second research question (Why do incidents happen and what events or conditions cause or increase the probability of IT service incidents?), we concentrated on events, event sequences, conditions and other contributing factors leading to an incident. We identified event sequences and a hierarchy of contributing factors to an incident (Paper IV). The probabilistic relationships of these contributing factors were studied (Papers V).

Regarding the third research question (What events or conditions during the incident lengthen its duration or increase the impact of it?), we identified an event called the incident within an incident, which lengthens the duration of an incident (Paper IV).

The fourth research question (How could the incidents in the ITSM operating environment be modelled to aid in proactive problem management, root cause analysis and CSI?) led us to develop an IT Incident Model (IIModel) consisting of a taxonomy, a charting method for events and causal factors (Paper IV) and a BBN (Paper V) to calculate the risks and aid in the root cause analysis. The BBN model was populated by categorized root causes and their causal relationships. This model enables IT organisations to see the probabilities of background causal factors, to a given root cause. On the other hand, the BBN
calculated a new root cause distribution, when contributing factors were changed.

A cyclic proactive problem management process was developed as a framework for the IIModel (Paper III and this thesis).

### 8.2.2 Implications to research and to practice

Implications for science include enhancements to earlier incident models by developing an incident model adapted to the ITSM. All three major parts of the model (i.e. taxonomy, SECFC presentation, using BBNs) include challenging existing incident models and practices or developing new models or practices.

The most important framework, ITIL, does not address the hierarchical nature of causal factors, described in the taxonomy part of the model. The SECFC part of the model is compatible with the extended lifecycle description of the incident adding value to it. A new scientific observation was also the difference between the ITSM incidents and incidents in other industries. Therefore, this research could not effectively use the models and methods from other industries.

Implications for practice include a set of new tools for an incident investigator or the problem manager of an IT service provider. The MIA method helps in incident trend analysis to find the problematic domains in IT services. MIA should be used in the data collection phase. It helps in the hypothesis generation and analysis phases. The taxonomy and SECFC are useful tools in data collection, hypothesis generation, analysis, and the presentation of findings and recommendations.

The BBN adds a new dimension to the analysis of large numbers of existing incidents. Instead of traditionally analysing the direct root causes with their probabilities, the model enables the analysis of chains of events and conditions with their conditional probabilities. This feature makes the model suitable for a retrospective analysis of the occurred incidents, as well as a prospective, what-if analyses. The BBN tool is useful when planning a proactive problem management cycle pointing to the possible risky areas. It also helps in the hypothesis generation
phase by calculating conditional probabilities based on the current and previous information of incidents.

The financial losses, because of the IT service incidents, are several percent of GDP. Therefore, it is of utmost importance to find methods, tools and practices to reduce the amount of losses.

8.2.3 Future work
The origin of this work has been in practical, real life ITSM work. The deliverables are meant to help the daily work of an ITSM professional. Effective and efficient deployment would require training material and an incident investigators guidebook. The investigators work would be easier with better results, if a sample set of known causes and contributing factors would be included in the workbook.

The reliability of the model could be validated by an interrater reliability test, where several raters categorise the incident causes according to a given taxonomy.

The incident and root cause probabilities were evaluated with BBN. One could add more value to the BBN by including information about the frequencies of incidents, configurable items (Cis) and their relationships.

By adding an incident categorisation scheme to ITSM tools and incident and problem records, it is possible to generate a real time situational picture of incidents and their contributing factors and thus partially automate the proactive incident management process.

The Multidimensional Incident Analytics (MIA) was presented as a tool for an advanced incident and problem record log analysis in an incident trend analysis. An option for future work would be to study commonly used log analysis tools for an incident and problem analysis. Examples of these tools include Splunk and ELK (Elastic Search, Logstash, Kibana). If the root causes of the incidents were categorized and recorded directly in their respective records, these log analysis tools would provide the possibility to a real time dashboard, situational picture of the incidents.
References


Bilbro, J. 2013, An inter-rater comparison of DoD human factors analysis and classification system (HFACS) and human factors analysis and classification system—maritime (HFACS-M) classification system, Naval Postgraduate School.


Department of Defence 2005, 1. Department of Defense Human Factors Analysis and Classification System - A mishap investigation and data analysis tool, Department of Defense, USA.


Griffin, T.G.C., Young, M.S. & Stanton, N.A. 2015, Human Factors Models for Aviation Accident Analysis and Prevention, Ashgate Publishing Company, Brookfield, VT, USA.


Hollnagel, E., Pruchnicki, S., Woltjer, R. & Etcher, S. "Analysis of Comair flight 5191 with the functional resonance accident model".


International Monetary Fund 2015, World Economic Outlook Database, October 2015, Gross domestic product of United States and Canada, International Monetary Fund, Washington, D.C., United States.

ISACA 2012, COBIT® 5: Enabling Processes, ISACA, Rolling Meadows, IL, USA.


Jäntti, M. 2008, Difficulties in Managing Software Problems and Defects, University of Eastern Finland.


National Transportation Safety Board, Major Investigations6/5/2016].


Patterson, J. 2009, Human error in Mining: A multivariable analysis of mining accidents/incidents in Queensland, Australia and the USA using the human factor analysis and classification framework, Clemson University.


Quorum, I. 2013, *Quorum Disaster Recovery Report Q1 2013*.


Rasmussen, J., Svedung, I., Statens räddningsverk (Sweden), National Centre for Learning from Incident & Accidents Staff 2010, *Proactive Risk Management in a Dynamic Society*, Statens räddningsverk.


References


Southern California Safety Institute (SCSI) 2016-5-7-last update, *Certificate Program in Aircraft Accident Investigation (AAI)*.


Virtually all functions in modern society depend on information technology (IT) systems and their uninterruptible operation. This thesis aims to explain the typical root causes of unplanned IT service interruptions, incidents and what their contributing factors are. The IT service incident model (ITModel), other tools and methods are developed in order to understand the underlying conditions to incidents, prevent their reoccurrence and improve the IT service quality.