Creating an ITIL-based Multidimensional Incident Analytics Method: A Case Study

Kari Saarelainen
Management Consulting
KPMG Finland
Helsinki, Finland
e-mail: kari.saarelainen@kpmg.fi

Marko Jäntti
School of Computing
University of Eastern Finland
Kuopio, Finland
e-mail: marko.jantti@uef.fi

***Abstract*—Many IT organizations have recognized incident categorization as a challenge because there are no general policies or guidelines for incident categorization. This leads to incident categorization usually being seen as an optional task for the specialists who handle incidents. The research problem of this study is as follows: what type of incident and root cause categorization model would be efficient and would also support ITIL-based (IT Infrastructure Library) continual service improvement? The results of this study consist of two parts: First, the software incident and root cause categorization model, which helps an IT organization to categorize incidents and their root causes effectively and recognize the weak points of the IT service delivery, and second, the provision of the lessons learned for improving incident categorization and measurement practices. The research was conducted as a case study that was carried out in an IT service company.**

Keywords- IT service management; ITIL; continual service improvement; incident management, root cause; categorization

I. INTRODUCTION

IT service providers are constantly seeking more effective methodologies, processes and tools in order to optimize the efficiency and quality of the process. IT Infrastructure Library (ITIL) is the most widely used best practice framework for IT service management [1]. ITIL provides a set of guidelines for managing information technology (IT) infrastructure, development, and operations as well as addresses the quality of IT services in several different ways. The most notable quality concepts within IT service management are service level management, incident management, problem management processes and Continual Service Improvement (CSI), which is related to all the stages of IT service lifecycle. This study will focus on the Incident Management and Service Operation processes and CSI [3] lifecycle stage, which have given guidelines used within an action research cycle.

The purpose of incident management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations [2]. Problem management seeks to minimize the adverse impact of incidents and problems on the business that are caused by underlying errors within the IT Infrastructure. Problem management process is invoked, e.g., if similar types of incidents are recurred or a major incident has occurred and the root cause needs to be analyzed. Root causes can also be divided in categories. Incidents are categorized in incident logging by service desk personnel. This category can be changed during incident management process. The category in this phase usually involves the selection of service, activity, type, function or configuration item (CI) and answers the question “what”. Root cause is the output of problem management and answers to the question “why”.

In this study, we gather data from a fairly large number of incidents, which have their root cause analysis activities made and reports written. Using attributes available (incident category, root cause category, location, incident duration, date, responsible, etc.) and simple analysis tools we are able to, in most cases, to point statistical deviations, which helps to recognize the weak points of services and processes. Most of the attributes above are fairly standard, and the measurement is unambiguous independent of person, country, and organization, e.g., date, time, duration, etc. Incident and root cause categories, are however, not described in IT service management standards such as in ISO/IEC 20000 [4] or frameworks such as ITIL and Control Objectives for Information and Related Technology (COBIT) [5]. In order to statistically analyze or otherwise identify recurring incidents or incident types or root cause types, the incident and root cause categories must be agreed and defined.

A. Related work

Previous research on incident management has addressed the importance of incident classification. Caldeira and Brito e Abreu [6] have used statistical methods to analyze product related incidents. Jäntti and Kalliokoski [7] have identified challenges related to service desk work and reported that service desk staff had problems in finding and selecting a correct Service Level Agreement and configuration item for incidents. Dan et al. [8] use business driven IT management and risk decision making theory to prioritize incidents. One of the key objectives of the incident categorization activity is to provide information for identifying the same type of incidents or incidents that are caused by the same root cause. Do Mar Rosa et al. [9] have used incidents to identify provided IT services for the organization’s service catalogue. Marcu et al. [10] have presented an incident correlation model based on category-based correlation aiming at identifying similar incidents by automating the process. Cusick and Ma [11] discuss how incident management approach (including single point of contact and escalation procedures) was established in a service provider organization.

ISBN: 978-1-61208-399-5

While in the IT service management the problem management process is responsible for investigating the root cause of incidents by Root Cause Analysis (RCA), in Software Engineering this activity is called a Defect Causal Analysis (DCA). DCA [12] aims at identifying causes of defects in order to prevent defects or to find them earlier. Defect prevention activity is also included in Capability Maturity Model (CMM) [13].

DCA typically includes causal analysis meetings, group meetings, that focus on identifying root causes as well action team meetings. Software Engineering Institute has introduced a Framework for Counting Software Defects and Problems [14]. This framework provides description how to classify problems and defects. In the Personal Software Process [15], the defect collection method includes a defect classification scheme and defect attributes. According to Jäntti et al. [16], IT organizations seem to have remarkable difficulties in managing defects and problems. In our study, we highlight the role of improving incident analysis.

B. *Our contribution*

The main contribution of this paper is an incident and root cause categorization model. The purpose of this model is to locate and point weaknesses in IT service delivery as a part of CSI.

This categorization can be used in service improvement efforts that are done as one-time exercises, as part of regular service quality reviews or as on-going activities integrated in ITSM systems. The purpose of the model is to help IT organization to identify the weak areas (people, process, technology, etc.) in IT service management, that are usually sources of identified root causes.

The rest of the paper is organized as follows. The research problem and methods are described in Section 2. The creation and validation of the incident and root cause categorization model is covered by Section 3. The analysis of the findings is covered in Section 4. The conclusion in Section 5 summarizes the case study.

II. RESEARCH METHODS

The research problem in this study is: How incident and root cause categorization can be used to support CSI. This qualitative research study was built using the case study and action research methods. The research problem was divided into the following research questions:

RQ1: What type of information can be used in creating an effective incident and root cause categorization model?

RQ2: How the combination of incident and root cause categories could be used for trending of incidents.

RQ3: What other incident related attributes could be used for more effective incident trending and other IT service improvement activities.

A. *Case Organization and Data Collection Methods*

The research was conducted in 2012 – 2014 on several distinct occasions reflecting several customers and several types of environments. All of these service environments were maintained by a single IT service provider, later the case organization. Multiple data collection methods proposed by Yin [22] were used during the study and the following data sources were used:

- **Participant observation:** Meetings and discussion with managers.
- **Interviews**: Interviews of roles responsible of services offered to customers and interviews of experts of service provider involved in the incident
- **Documents:** Incident reports, process descriptions, work guides and guidelines
- **Records and archives:** Change, incident and problem records.
- **Physical artifacts:** ITSM tool.

The research followed the action research cycle as proposed by Baskerville [23]. The five phases of this cycle are presented in Fig. 1: A. Diagnosis, B. Action Planning, C. Action Taking, D. Evaluation, E. Specifying Learning.

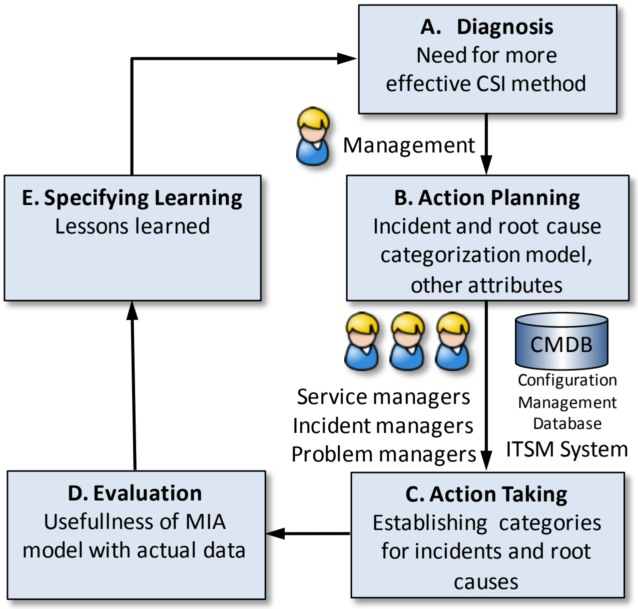

A. Diagnosis
Need for more effective CSI method
Management
E. Specifying Learning
Lessons learned
B. Action Planning
Incident and root cause categorization model, other attributes
CMDB
Configuration Management Database
Service managers
Incident managers
Problem managers
ITSM System
D. Evaluation
Usefullness of MIA model with actual data
C. Action Taking
Establishing categories for incidents and root causes

Figure 1. The Action Research Cycle in this research

B. *Data Analysis Methods*

The data of this action research study were collected and analyzed using a within case analysis technique [17]. The incident categorization scheme and findings were validated through discussions and improvement workshops with the representatives of the case organization. The principal author was responsible for producing a summary of findings that was delivered to the case organization. The established incident categories were improved taking into account the comments from case organization's managers and some new categories were added to the original classification.

III. RESULTS

As main results, we document the action research cycle that focused on improving the categorization of IT service incidents. The action research resulted in a method for analyzing incidents with multiple attributes. This method is called Multidimensional Incident Analytics (MIA).

A. Diagnosis

The diagnosis phase aims at identifying the primary problem, which needs to be solved through action research. This phase started by organizing a meeting with the case organization's management. The objective of the management was to check the current state of IT service delivery and identify improvement areas.

The case organization's management requested a more effective method for continual service improvement of IT services. There are several alternative and complementary methods to approach the improvement. The management chose the improvement based on analysis on those incidents, from which there has been a separate incident report including root cause analysis.

B. Action planning

The action planning phase specifies organizational actions to solve and investigate the problem identified in diagnosis phase. The action planning phase started with designing the incident analysis method. According to ITIL framework, incident categorization can be used for incident analysis for, e.g., establishing trends for use in proactive problem management and other service improvement activities, as well as measuring the performance of incident management. This method sorts the incidents mainly according to chosen incident category.

There are, however, several other attributes, which can be connected to the chosen incident. If these attributes are in numerical format or they are lists with a defined set of values, one can apply data analytics methods on them.

Root cause is one of the most useful attributes. The incident record usually contains also other potentially useful information for incident analysis, for example date and time of incident, duration of the incident, CI (this may also the basis for incident categorization), priority, impact, and relationship with other CIs, incidents, problems, changes or known errors. Other sources for attributes of incidents to be analyzed include monitoring and capacity information, and application portfolio attributes.

In order to keep the data manageable, incident category, root cause and occurrence data and time were chosen incident attributes to be analyzed. The incident reports were not in the standard format, and especially the root causes were free-form textual descriptions. For analysis purposes relevant incident and root cause categories were to be developed.

1) Incident categories

In general, incident category answers the question "**what** (was impacted by the incident)". It can be used to support proactive problem management activities such as trend analysis and the targeting of preventive action. Identified problems from these activities will be used in continual service improvement activities. In ITIL framework [2], an incident is defined as "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". A root cause is "the underlying or original cause of an incident or problem". Problem management process is responsible for the resolution of the root cause.

All incidents should have a standard category schema. This provides faster access to incident and troubleshooting information, and also better support proactive incident trending. Since organizations are unique on the categories, it is hard to find a universal set of categories, especially on the detailed level. ITIL proposes the following generic steps for incident categorization [1]:

1 Hold brainstorming sessions with stakeholders.
2 Generate the initial main categories incl. 'other'.
3 Use the main categories for a short trial period.
4 Analyze the incidents logged during the trial period. The number of incidents logged in each category will confirm if the category was successful. If the number of incidents is high in 'other' category, consider creating a new main category.
5 A breakdown analysis of incidents in main categories tells, if subcategories are required.

2) Root cause categories

Root cause categories answer the question "**why** (the incident happened)". For proactive problem management sole incident category inspection is a not a very powerful tool. Several root causes may cause symptoms that may be spread across several incident categories. For example, human errors, facility problems (electricity, cooling, humidity), supervisory, guidance and process problems typically cause incidents in several different incident categories. Incident and root cause categories can be considered orthogonal, independent from each other. Virtually all the root cause categories can exist in all the incident categories.

In literature, root cause classification or categorization is handled very little. Where root cause categories are handled, it is done in other domain, e.g., in nuclear plant context [21], independently of domains [18] or only one main category of root causes, e.g., human factors [20]. Generally the root cause analysis methods [1][18][19]][21] and categories can be used also in other domains or they can be used as a basis of root case category development. There is no guidance in root cause categorization in ITIL unlike in incident categories. As a phenomenon it is similar to incident category, and the researchers decided to handle it with the same procedures as in incident categories.

3) Other attributes

Other potential incident attributes from incident records, changes, CIs, other related incidents, problems, changes or known errors, monitoring and capacity information, and application portfolio were not systematically studied. If this information existed in the incident report, it was taken into account when drawing conclusions and proposing improvements. Starting time of the incident was, however, taken as an attribute. Starting time made possible to place the incident on a time line and in correlate it with other events at the same time.

Information about the responsible party was left as an attribute. This is often a big question in an incident, especially if penalties are to be paid because of service level breaches. The conclusions and recommendations are also different, if the incident was because of actions of customer or subcontractor rather than the actions of IT service provider itself. The attribute responsible party answers the question ”**who** (was responsible)”.

C. Action taking

The action taking phase focus on implementing the planned action.

1) Establishing incident categories

The case under study was a company internal quality improvement effort. The purpose was to collect a representative amount of incident reports, where the root cause was analyzed. Since this was a set of separate reports and not incident tickets there were no obligations to follow the allocated categories in incident records. The researchers were free to choose the categories, which suited best to service improvement activities.

ITIL encourages using multilevel categorization, which is also supported in most ITSM systems. Examples of typical categories of requests include:

- **By service:** For example, a request to create a new user email account may be part of an email service.
- **By activity:** For example, password reset, laptop installation or printer cartridge replacement.
- **By type:** The request is categorized by its type, e.g., an informational request and a standard change.
- **By function:** For example, service desk, technical management, IT operations management and application management.
- **By CI type:** The type of CIs that the request or event impacts.

The chosen category type reflects also who is providing and using that information and what is the strategy in incident trending. Customer of IT service or business may be more interested to categorize in business service terms incidents, which are visible in the customer interface. Then categorization by service or by activity may be more natural. If the objective is to measure and improve internal quality of IT service delivery, one usually takes categories close to internal organization (by function) or by CI type.

The environments included environments dedicated to customers and also shared by several customers. In all of these IT service delivery was organized as technology oriented teams, technical domains. The teams performed several processes and activities, e.g. change management, incident management, problem management, monitoring, etc. The organization of technical domains reflected the hierarchy of CIs. Because of all of these reasons it was a natural choice to take the responsibility areas of technical domains as starting point of main incident categories. After some trial exercises and iterations, the researches added couple of extra categories. Because the aim was not in this phase to create a global ongoing incident categorization for use in incident management process and with the ITSM system, no lower level categories were defined. The following incident categories were chosen:

- **Network:** All passive and active network devices including switches and firewalls.
- **Server:** Servers in general. Memory incidents were separated in a category of its own.
- **Memory:** Incidents in physical memory, e.g. lack of memory and physical memory errors
- **Storage**: Storage systems and storage networks.
- **Database:** Errors in databases.
- **Application:** Application service running in servers.
- **Integration/job processing:** Integrations and batch job between services.
- **Facility systems:** Electricity UPS, cooling, etc.
- **Other:** Incidents not fitting in other categories.

2) Establishing root cause categories

According to ITIL the operation of ITSM as a practice is about preparing and planning the effective and efficient use of the four Ps: the people, the processes, the products (services, technology and tools) and the partners (suppliers, manufacturers and vendors). These were chosen as a starting point. Since it was decided to establish a set of attribute answering the questions who, partners were moved to that attribute. After analyzing initial incident profiles, it was decided to split products into two subcategories: software and hardware. Since later it was suspected that a some server and network devices running certain operating systems were unreliable, a third device category was added: firmware.

Root cause categories:

- **Software:** bugs, malfunctions and configuration errors in applications.
- **Firmware:** bugs, malfunctions and configuration errors in firmware and operating systems of servers and network and security devices.
- **Hardware:** Malfunctions and errors in hardware, e.g. fans, CPU, memory, bus, cards, etc.
- **Process:** Poorly defined, implemented, communicated or supervised process, e.g. too loose change management process
- **Human error:** Something that was not intended by the actor thus causing the incident.
- **Other:** Any other root cause for the incident.
- **Unknown:** Root cause was not found or it was not analyzed.

*3) **Establi**shing responsible party categories*

The responsible parties were divided into following subcategories

- **IT service provider:** IT service provider self caused the incident.
- **Network operator:** The incident was caused by network operator.
- **HW/SW vendor:** The incident fell in this category, if hardware or software had bugs, and IT service provider could not avoid them, e.g. with updates according to recommendations.
- **Customer:** Incident was caused by erroneous actions or faulty information of customer.
- **Other:** Some other party caused the incident.

D. Evaluation

The evaluating phase aims at evaluation the outcomes of the action research. In our case we focused on evaluating usefulness of the MIA method.

After the data collection and categorization work the researches had 165 incident reports from different environments with enhanced incident records. From the point of view of this study the core attributes of the incident records were: incident category, root cause category, starting time of the incident, and responsible party. The tool used in this analysis was a spreadsheet application. One may, however, apply also more sophisticated tools, such as data analytics and BI tools in order to analyze incidents. With more sophisticated tools it is possible to study a larger set of attributes (dimensions).

E. Specify learning

In this study, we specified learning in the form of lessons learned. In the Specify learning phase organization identifies and creates knowledge gained during the action research. Both successful and unsuccessful actions enable learning. The following lessons learnt were derived.

Lesson 1: Incident and root cause logging, categorization and analysis should be one part of CSI. The analysis of theoretical frameworks showed that incident logging is part of operative incident management, while incident root cause analysis is performed in problem management. Our empirical findings suggest that it might be useful to include the root cause of incident also in the incident record but at least in the problem record. Adding additional dimensions to incident analysis may bring essentially more accuracy and efficiency to high level incident analysis.

Lesson 2: Root cause categories are needed. Root causes are not typically categorized, when they are analyzed and logged. The root causes are rather described only in free text form if at all logged. In order to perform systematic analysis root causes should also be categorized in the same way as incident categories.

Lesson 3: Investigate human errors. Investigation of root causes revealed a significant number of human errors.

Lesson 4: Improvements in incident classification may reflect to other ITSM processes. Incident categorization triggered improvements in change management process.

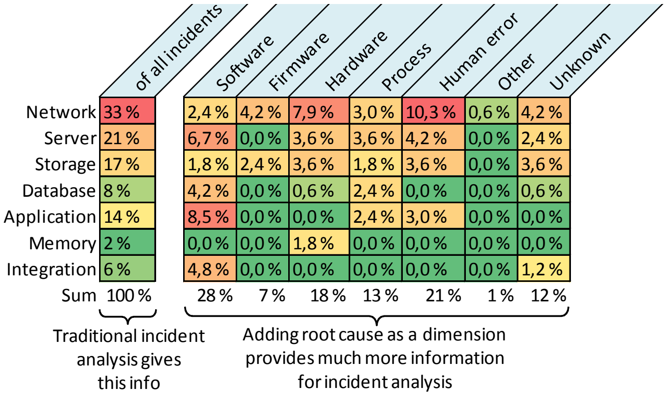
Lesson 5: Clarify the difference between categorization and classification. The difference between categorization and classification is unclear to the ITSM practitioners. Our theory-based findings show that ITIL v2 used a term classification while ITIL v3 used categorization and prioritization.

Lesson 6: Capture multiple root causes. Ensure that the tool is able to capture multiple root causes in IT service management tool. Root cause changed in appr. 30% of cases after interviewing the persons involved with the incident.

IV. ANALYSIS

The analysis phase started by establishing a two-dimensional analysis (incident category – root cause category) for IT service incidents. The correlation of incident categories with root cause categories answered the question, whether the some of the root cause categories was dominant in some of the root cause categories. Example is presented in Fig. 2. Traditionally, the incidents are inspected in one dimension. Adding root causes to incident categories improves essentially the accuracy of the analysis (see Fig. 2). E.g. in the example we see that 33% of all errors are network errors. The other columns allocate this figure in root cause categories. Now we see, that 10,3 % of network incidents are because of human errors and 7,9% hardware problems and 4,2% firmware problems. Excessive human errors can be handled, e.g. with tighter change management, training, supervision, etc. Firmware errors may be mitigated, e.g. by paying attention to use proven versions of the software. One may also consider other vendors, especially, if the hardware problems were caused by the vendor.

The analysis above could be done to each environment. Environments may also easily be compared with each other or the baseline consisting of all environments.



	of all incidents	Software	Firmware	Hardware	Process	Human error	Other	Unknown
Network	33 %	2,4 %	4,2 %	7,9 %	3,0 %	10,3 %	0,6 %	4,2 %
Server	21 %	6,7 %	0,0 %	3,6 %	3,6 %	4,2 %	0,0 %	2,4 %
Storage	17 %	1,8 %	2,4 %	3,6 %	1,8 %	3,6 %	0,0 %	3,6 %
Database	8 %	4,2 %	0,0 %	0,6 %	2,4 %	0,0 %	0,0 %	0,6 %
Application	14 %	8,5 %	0,0 %	0,0 %	2,4 %	3,0 %	0,0 %	0,0 %
Memory	2 %	0,0 %	0,0 %	1,8 %	0,0 %	0,0 %	0,0 %	0,0 %
Integration	6 %	4,8 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	1,2 %
Sum	100 %	28 %	7 %	18 %	13 %	21 %	1 %	12 %

Traditional incident analysis gives this info
Adding root cause as a dimension provides much more information for incident analysis

Figure 2. Example of incident category - root cause analysis.

We found that improvements in incident classification triggered improvement of other ITSM processes. This supports the findings of a previous study [7], where improvement of classification led to improvement of service level management. Our findings also support the findings of an existing defect management study [16] that proposed that organizations have difficulties in managing problems and defects. One of the major difficulties is defect classification.

It seems that traditional defect classification models, such as classification scheme of Personal Software Process are mixtures of software development lifecycle activities, architecture and infrastructure building blocks [15]. These are useful in the IT service design and transition phases, but don't fit in the IT service operation phase. The IT service operation phase emphasizes services, where products in maintenance phase are in production use in a given environment. We propose that IT service management could benefit from continuous root cause analysis and MIA as a CSI method. Additionally, service oriented classification models have some unique features that software oriented classification models lack, such as service level agreements.

V. CONCLUSIONS AND FUTURE WORK

The research problem in this study was: What type of incident and root cause categorization model would efficiently support ITIL-based continual service improvement. The unit of the study was a Finnish IT service provider company and its incident management process.

The research was conducted according to the phases of the action research cycle. The main contribution of the study was to describe how a MIA model was designed, and what was learned during the action research.

There are certain limitations related to this study. First, action research typically includes several iterative research cycles. However, we focused on describing only one improvement cycle that focused on improving the analysis of IT service incidents. 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 style problem solving. Third, regarding method triangulation, we could have used organizational change theory more extensively to support our technology- and process-based problem solving approach.

Future research could aim at refining our MIA model by adding new dimensions to it, as well as exploring the root cause category models based on IT service management practices.

ACKNOWLEDGMENT

We would like to thank the case organization's representatives for valuable feedback and responses that helped us to perform this study.

REFERENCES

[1] Cabinet Office, ITIL Service Strategy. The Stationary Office, UK, 2011.

[2] Cabinet Office, ITIL Service Operation. The Stationary Office, UK, 2011.

[3] Cabinet Office, ITIL Continual Service Improvement. The Stationary Office, UK, 2011.

[4] ISO/IEC 20000:1, Part 1: Service management system requirements. ISO/IEC JTC 1 Secretariat, 2010.

[5] COBIT 5, Control Objectives for Information and related Technology: COBIT 5: Enabling Processes. ISACA, 2012.

[6] J. Caldeira and F. B. e Abreu, "Influential factors on incident management: Lessons learned from a large sample of products in operation," in Product-Focused Software Process Improvement, A. Jedlitschka and O. Salo, Eds., vol. 5089. Springer Verlag, 6 2008, pp. 330–344.

[7] M. Jäntti and J. Kalliokoski, "Identifying knowledge management challenges in a service desk: A case study," in Proceedings of the Second International Conference on Information, Process, and Knowledge Management, eKNOW 2010. St. Maarten, Netherlands Antilles: IEEE Computer Society, February 2010, pp. 100–105.

[8] W. Dan, Z. Zhiqiang, and S. Hao, "An incident prioritization algorithm based on BDIM," in Proceedings of the ICCMS '10. Second International Conference on Computer Modeling and Simulation, 2010., vol. 3, Jan 2010, pp. 536–540.

[9] M. do Mar Rosa, N. Gama, and M. da Silva, "A method for identifying IT services using incidents," in Eighth International Conference on the Quality of Information and Communications Technology (QUATIC), 2012, Sept 2012, pp. 172–177.

[10] P. Marcu, G. Grabarnik, L. Luan, D. Rosu, L. Shwartz, and C. Ward, "Towards an optimized model of incident ticket correlation," in IFIP/IEEE International Symposium on Integrated Network Management, 2009. IM '09., June 2009, pp. 569–576.

[11] J. Cusick and G. Ma, "Creating an ITIL inspired incident management approach: Roots, response, and results," in Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, April 2010, pp. 142–148.

[12] D. N. Card, "Learning from our mistakes with defect causal analysis," IEEE Software, vol. 15, no. 1, pp. 56–63, January/February 1998.

[13] CMMI, Standard CMMI Appraisal Method for Process Improvement (SCAMPISM) A, Version 1.3: Method Definition Document. USA: Software Engineering Institute, Carnegie Mellon University, 2011.

[14] W. Florac, "Software quality measurement a framework for counting problems and defects," Technical Report CMU/SEI-92-TR-22, 1992.

[15] I. Hirmanpour and J. Schofield, "Defect management through the Personal Software Process," Crosstalk, The Journal of Defense Software Engineering, 2003.

[16] M. Jäntti, T. Toroi, and A. Eerola, "Difficulties in establishing a defect management process; a case study," in Proceedings of the 7th International Conference on Product-Focused Software Process Improvement, ser. LNCS 4034, J. Munch and M. Vierimaa, Eds. Amsterdam, The Netherlands: Springer-Verlag, Berlin Heidelberg, June 2006, pp. 142–150.

[17] K. Eisenhardt, "Building theories from case study research," Academy of Management Review, vol. 14, 1989, pp. 532–550,.

[18] Paul F. Wilson, Root cause analysis: A Tool for Total Quality Management, ASQ Quality Press, Jan 1, 1993.

[19] Lee N. Vanden Heuvel and Donald K. Lorenzo, Root Cause Analysis Handbook, Rothstein Associates Inc., Brookfield, Connecticut, USA, 2008.

[20] Wiegmann, D. A., & Shappell, S. A., A human error approach to aviation accident analysis: The human factors analysis and classification system, Burlington, VT: Ashgate Publishing, Surrey, United Kingdom, Ltd, 2003.

[21] Doe guideline – Root cause analysis guidance document (DOE-NE-STD-1004-92), U.S. Department of Energy, Office of Nuclear Energy, Office of Nuclear Safety Policy and Standards, Washington, D.C., USA, 1992.

[22] Robert Yin. Case Study Research: Design and Methods. Beverly Hills, CA:Sage Publishing, 1994.

[23] Baskerville, Richard L. "Investigating Information Systems with Action Research," Communications of the Association for Information Systems: Vol. 2, Article 19,1999.