The Anatomy of IT Service Incidents

Kari Saarelainen
IT advisory
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*—An IT service is by definition "made up of a combination of information technology, people and processes". These elements, in addition to external factors, are also the key components of IT service incidents. This paper presents an integrated model of IT service incidents. This model extends the concept of root cause also to latent, contributing conditions to an incident. Additionally, the life cycle of an incident is presented in the model. Unlike incidents and accidents in other industries, an IT service incidents has a duration. The damage caused by an incident is proportional to this duration. In our study, we show that there are events and conditions during the incident, incidents within incidents, which cause delays in service restoration. The model is validated by a case study method using 15 incident descriptions to validate both the latent factors contributing to the direct root cause as well as the life cycle of an incident. The main contribution of this study is the incident model containing latent conditions and events contributing to the direct root cause and concept of incident within incident. The model improves the traditional root cause analysis and acts as a framework in IT service incident root cause categorization.**

***Keywords*—IT service management; ITIL; continual service improvement; root cause; categorization.**

I. INTRODUCTION

Most of the vital functions are dependent on the availability and quality of IT services. Critical IT systems are often committed to deliver 99.9% - 99.999% availability meaning monthly downtime from 43 minutes to 26 seconds. At the same time, the IT service production environment is growing more complex. The service quality and availability is controlled by a set of IT service management (ITSM), risk and security management processes and practices, as well as by processes related to organizational governance. IT infrastructure library (ITIL) [1] is the most common framework for ITSM processes. There are several processes in ITIL, which would benefit from a comprehensive model of IT service incidents:

- Incident trend analysis in proactive problem management. Incident trend analysis needs a solid basis for incident root cause categorization.
- Availability management focuses on reliability and on how to put in place alternative options to ensure the service continues. It is crucial to recognize the potential areas causing unavailability.
- Service level management focuses on delivering IT services with agreed quality.
- Continual Service Improvement (CSI) is a stage in the lifecycle of an IT service, which identifies and implements improvements.

A. *Swiss Cheese Model and latent conditions*

James Reason's Swiss Cheese Model (SCM) [2][3] explains the accident and incident as a result of long standing conditions and latent failures contributing to the unsafe act. The model is often described as a sequence of planes, cheese slices, which describe organizational levels, defenses and barriers of incidents. Failures (holes in cheese slices) can emerge at anyone of these levels. When the holes are at the same time in the same trajectory, the incident is likely to occur (Figure 1).

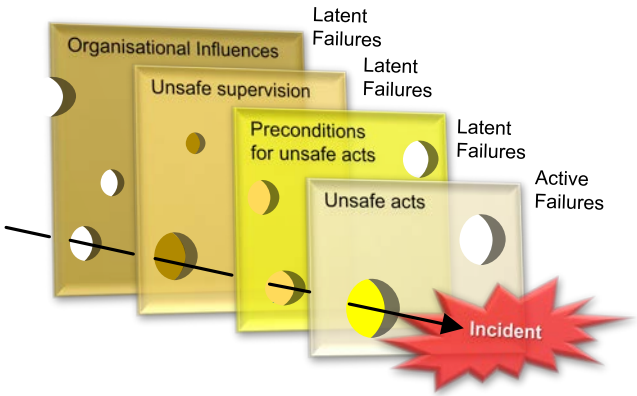

Figure 1. Swiss Cheese Model (SCM) of incident causation with HFACS taxonomy [3]

Wiegmann & Shappell [4] showed that many incidents have their roots high within the organization. Decisions made by top level management often influence the middle level management, as they supervise daily operations of the organization. The Human Factors Analysis and Classification System (HFACS) describes the taxonomy of human errors as well as the causal relationship between the unsafe act and the latent conditions behind it (Figure 2). HFACS has its origin in aviation, but it has adaptations in a broad range of other industries. Related to ITSM, HFACS is discussed in the studies [3][5][6]. HFACS, however, has some shortcomings in general and also when applied in ITSM.

- HFACS is a complex system. In aviation, where accident investigation may take weeks or months, complexity may be justified. In ITSM, service incidents are investigated in hours or days at most.
- HFACS has its roots in aviation, which is visible in its design. A model more adapted to IT work flows and ITSM environment is needed [6].
- HFACS covers only human factors. This may be justifiable in other industries, where human factors

 ISBN: 978-1-61208-451-0

cover 60-96% of incidents (Table I), but in IT the share of human errors is only 21-24%.

- The concept of incident in IT differs from the other industries. In ITIL, an incident is defined as "An unplanned interruption to an IT service or reduction in the quality of an IT service." When the service or service level is restored, the incident is over.

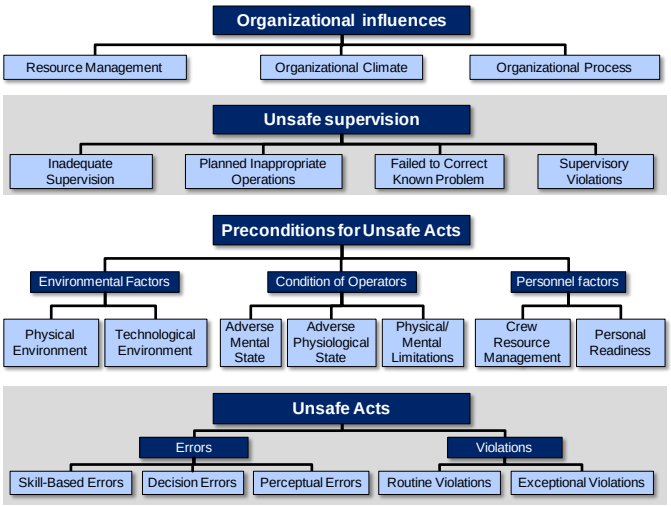

Figure 2. Hierarchical HFACS taxonomy of human factor contribution on incidents and accidents [6].

TABLE I. PROPORTION OF HUMAN ERRORS OF ROOT CAUSES OF INCIDENTS IN DIFFERENT INDUSTRIES

Industry	Human errors	Source
Aviation	70-80%	[7]
Maritime	75-96%	[8]
Railway	61 %	[9]
Healthcare	70-80%	[10][11]
Pharmaceutics	80 %	[12]
Nuclear energy	80 %	[13][14]
Chemical industry	60-90%	[15]
Telephony and Internet	19%	[16]
ITSM	18-24%	[17][18][19][22][23]

B. Other incident models and root cause analysis methods

There have been very few studies about IT service incidents, their causation, and incident models or frameworks.

Hinz [20] has studied causal modelling of end user computing. He has proposed some underlying factors, which increase probability of incidents with end users including hardware and software complexity, standardization, and maturity. The model, however, is limited to end user computing, the coverage of latent factors is rather limited, and leaves open the reasons to these underlying, latent factors.

Hazard and operability study (HAZOP) [20][29] is a process for identification of potential hazard & operability problems caused by deviations from the intended design. It was initially developed to investigate chemical production processes. HAZOP is also used for complex software systems [31]. HAZOP is, however, more a brain storming technique for system examination and risk assessment. It is a general purpose technique without ITSM specific parts. The technique finds best the direct risks and does not encourage to analyze the underlying conditions increasing the risk of incident.

ITIL presents 11 common root cause analysis (RCA) methods, which are given as examples [1]. Only two of them, namely 5-Whys and chronological analysis, address contributing causes to the direct root cause to some extent.

5-Whys RCA method works by starting out with a description of what event took place and then asking 'why this occurred'. The resulting answer is given, followed by another round of 'why this occurred'. Usually by the fifth iteration, a true root cause will have been found. 5-Whys does not, however, give a framework, 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.

Chronological analysis RCA method focuses on the timeline of events in order to see, which events may have been triggered by others. This method addresses clear, identified events, but misses the latent long lasting conditions. Also, it does not give a framework of formation of incidents.

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 model is covered by Section 3. The analysis of the findings is covered in Section 4. The conclusion in Section 5 summarizes the study.

II. RESEARCH METHODOLOGY

The research problem in this study is: How the incidents in ITSM operating environment could be modelled in order to aid proactive problem management, root cause analysis and continual service improvement. The research problem was divided into the following research questions (RQ):

RQ1: HFACS brings an idea of latent conditions contributing to the incident related to human errors. Can this model be extended to technology and processes?

RQ2: What are the major differences in concept of incident in ITSM and in other industries?

RQ2: How these possible differences with the concept of incident should be taken into account in the model?

A. Data Collection Methods

Information of IT service incidents was collected in 2011 – 2014 from incident reports provided by an IT service provider organization. Incidents reflected issues from several customers and different types of environments. Multiple data collection methods proposed by [21] were used during the study and the following data sources were used:

- **Participant observation:** Meetings and discussions with managers, observation of service desk work.
- **Interviews**: Interviews of roles responsible of services offered to customers and interviews with service managers and experts involved in the incident
- **Documents:** Incident reports, process descriptions, work guides and guidelines
- **Records and archives**: The incident report pool included 215 incidents. From this pool, all the reports with three of more identified root causes or

 ISBN: 978-1-61208-451-0

contributing events or conditions were chosen. The number of these analysis units was 15.

- **Physical artifacts:** ITSM tool.

B. *Data analysis*

All the 215 incident reports were studied, and root causes, contributing events and conditions, and 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 above. The model was build using the analyzed data and the fundamental ideas in Swiss cheese model and HFACS. 15 chosen incident reports were then applied to its model.

III. RESULTS

The main contribution of this paper is a comprehensive model of IT service incident for proactive and reactive problem management and risk management. In this section, we first present the model with its rationale and then apply it to the incident reports.

The model introduces latent factors and events contributing to the direct root cause. Additionally, it describes the lifecycle of incident containing the concept of *incident within incident.*

A. *The incident model*

1) *Top level root cause categories*

An IT service is by definition "made up of a combination of information technology, people and processes." [1]. These basic building elements of an IT service are also the major candidates for upper level root cause categories. Publicly available statistics of root causes usually omit processes, but add different external factors (e.g., forces of nature, cybercrime, etc.) to root cause categories (See Table II).

TABLE II. STUDIES OF ROOT CAUSES IN IT SERVICE INCIDENTS.

Source	Year	Technology	Human	External
Gartner/Dataquest [22]	1999	67 %	18 %	8 %
Enisa [16]	2014	66 %	20 %	14 %
Ponemon [18]	2013	58 %	22 %	30 %
Quorum [23]	2013	73 %	22 %	5 %

ITSM and other processes coordinate task flows performed by people and technology. If the process fails, the direct root cause is related to people or technology, not to process. The flaw in the process is a contributing factor in the background, and this is not usually gathered in statistics.

Figure 3 presents technology, human and external factors as direct root causes and processes in the background. Note, that the relevant process sets are different in external, technology and human factors. External factors are not controlled and managed in the same way as internal factors. One cannot set performance objectives or improve the quality of forces of nature or cyber criminals. The processes used to manage external factors include security, risk, availability and service continuity management. Architecture and procurement practices are unique to technology factors and leadership and HR processes are related to people. The incident root cause can be considered as a combination of several different factors (see Figure 3).

The idea of contributing factors has been presented by Reason [2] and later refined by Wiegmann and Shappel. [4], although restricted to human factors and originally in aviation industry.

Note that both direct causes and other contributing factors may be considered as root causes, which are by definition "the underlying causes of an incident or a problem, which if corrected would prevent or significantly reduce the likelihood of the incident's reoccurrence" [5].

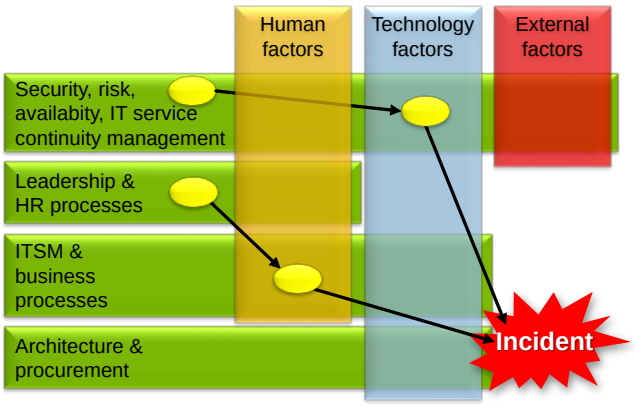

Figure 3. According to incident model presented in this paper, IT service incidents are caused by human, technology and external factors often contributed by failures in the background processes and practises.

2) *Causal levels*

The model consists of three incident root cause levels with causal relationship: Direct causes leading directly to incident, conditions to direct causes increasing probability of the incident, and organizational processes, policies, principles and practices contributing formation of conditions (Figure 4). Identifying these underlying factors helps identifying improvement possibilities in incident investigation and thus helping in making process improvements in CSI [3].

a) *Processes, policies, principles, practices (PPPP)*

Activities in an organization are guided by different processes, policies, principles and practices. In addition to ITSM processes, there are human resource and procurement policies, rewarding and motivations systems, architectural principles, cultural issues, etc. The category list of root causes in Figure 4 is not meant to be exhaustive: The difficulty of defining thorough category lists is visible already in ITIL: IT service management was handled with 10 processes by ITILv2 (2001) [24][25], while ITILv3 (2007, revised 2011) uses 30 processes and functions [26].

b) *Inadequate conditions*

Failures at PPPP causes inadequate design or behavior, which increases the probability of an incident.

Technology conditions: In technological environment failures in architecture may create complex, error prone systems. Flaws in risk calculations, and in availability management may cause non-resilient systems. Problems in procurement and IT operations & management may result in non-standard devices purchased from different sources and managed manually. Financial situation may result in savings in personnel, tools or system redundancy. In Figure 4, the maturity, standardization and complexity, design, maintenance and suitable tools are contributing technical conditions. Maturity, standardization and complexity are contributing technical conditions proposed by Hinz [20]. Other categories were extracted from the cases in this study.

 ISBN: 978-1-61208-451-0

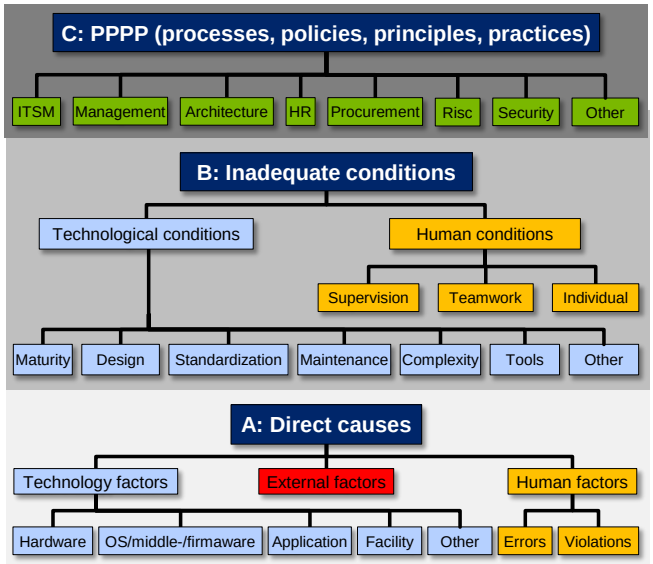

Figure 4. Causal levels of IT service incidents with indicative root cause categories in each level.

Human conditions: Saarelainen and Jäntti [3][6] have studied IT service incidents in matrix organization typical in IT service providers. According to these results, the human conditions in the model have dimensions reflecting line management (supervision) and processes (teamwork) in a matrix organization as well as individual readiness (training, cognitive factors, mental and physical state).

Note that not all the conditions are caused by PPPP. Technical devices have a measured and/or calculated mean time between failures (MTBF) that is one of the key reliability metrics within IT service availability management [27]. People may have mental or physical disabilities and behavioral features, which are beyond the control of PPPP.

c) Direct causes

Direct causes trigger the incident. They are usually reported as root causes in incident reports.

Technology factors: Technology factors are usually divided in hardware and software. Software related root causes are often further divided in operating system, firmware, middleware and application. Most ITSM root causes belong to technology factors (Table II).

Human factors: Wiegmann and Shappel [7] have made pioneering work in categorization of human errors and modelling contributing conditions. Their HFACS model as such seems to be too complex for ITSM. Having its roots in aviation it also needs adaptation to ITSM environment [3]. In this model the categories Human conditions and Human factors contain elements of HFACS simplified. At "direct causes" level human errors are categorized as unintentional (errors) or intentional (violations) by HFACS.

External factors: External factors is an umbrella term to all the factors that are beyond internal controls and process improvement efforts of the organization. Thus, they are managed only by security, risk, availability and IT service continuity management processes but not by other ITSM or business processes. If an external party, e.g., subcontractor participating in ITSM processes, it is considered non-external in this model. External factors include, e.g., vandalism, cybercrime, denial of service attacks, cable theft, flood, wind, snow/ice, lightning, other forces of nature, etc.

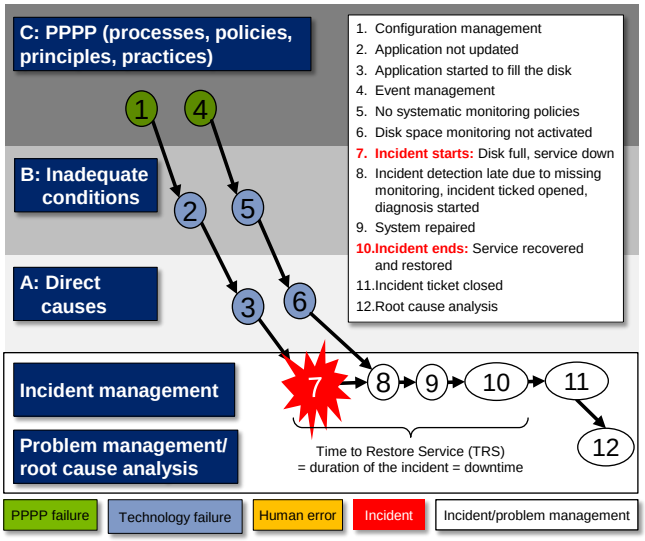

Figure 5. Extended life cycle of the incident nr. 9 in the text. The colors of background and events/conditions are as in Figure 4.

d) Incident life cycle

Traditionally, in other industries the incident or accident is over, when the damage has occurred. In ITSM, this is only the beginning of the incident (Figure 5) [27]. In point 7, the incident has taken place, in point 8 it is identified and the incident record is created (the ticket is opened) and diagnosis has started. In point 9, the system is repaired, and in 10 the service is restored. The time between points 7 and 10 is called Time to Restore Service (TRS). This is also the lifetime of the incident. If the incident causes service breaks, this period is called downtime.

3) Events before and during the incidents

The original hypothesis in this paper was related to the actual incident and events and conditions leading to it. Almost 50% of the cases under study, however, contained events and conditions that delayed the service recovery.

The core contribution of this paper is, what happens before and during the incident, and why it happens (points 1-6 in Figure 5). Figure 5 presents one case in this study, where the incident was directly caused by a software bug in applications, which started to fill the disc (point 3). This bug in turn was a known bug in an outdated version of the software (point 2). Leaving applications as outdated versions is one probable result of immature configuration management. Additionally, a failure occurred during the incident, which increased the incident duration. The detection of incident was delayed (time between points 7 and 8), because the disk was not under monitoring (point 6). Inadequate monitoring was a probable result of immature event management process (point 4), which is responsible for detection of events, including service failures. Usually, the IT service provider pays penalties stated in the service level agreement (SLA) according to cumulative service downtime. Thus, the damage to IT service provider caused by SLA penalties and also the damage to the customer caused by lost business is usually proportional to the length of the downtime or service degradation. By now, the focus in ITSM has been on direct root causes, not in contributing factors leading to this incident and not in factors increasing incident duration.

In the current ITSM practice, incident root cause analysis (point 12 in Figure 5) covers usually the direct cause of the

 ISBN: 978-1-61208-451-0

incident (point 3 in Figure 5, "Application started to fill the disk"). In this example, the usual root cause analysis approach leads to root cause "software bug". This gives a very moderate input to service improvement efforts. This study proposes that in IT service incidents root cause analysis should cover points 1-10. The latent, contributing factors leading to incident as well as contributing and direct factors slowing down service restoration should be covered in the analysis. In this example, a more extensive (points 1-10) root cause analysis approach would possibly lead to recommendation to revise configuration and event management practices.

B. *Validation of the model*

The model was validated using existing incident reports. According to our observations, the general quality of incident reports was poor. 27% (N=58) of the reports (N=215) had no identified root cause, 46% (N=99) had one root cause. 27% of reports identified two or more root causes/contributing factors. In this study, we selected all the cases (7%, N=15) with three or more identified root causes or contributing factors. Letters A, B and C in front of events/conditions refer to the causality levels in Figure 4.

1 **Unsuccessful disc space addition:** C: Configuration management -> B: Old SW version unable to repair file system -> A: File system got corrupted -> ***Incident***
2 **Network failure:** B: System was not designed redundant -> A: LAN Switch failure -> ***Incident***
3 **Unplanned service break:** C: Configuration management -> B: unsupported HW combination -> A: network failure -> ***Incident***
4 **Unsuccessful file transmission:** C: Poor instructions for testing in change management process description -> B: poor testing during the change -> A: file transfer did not work in different environment -> ***Incident*** -> A: no alarm of not successful file transfer -> ***Longer time to restore service (TRS)***
5 **Filled system log:** A: SW error -> A: System log getting full -> A: Wrong info is given to operator -> A: Log is full -> ***Incident*** -> A: Event is not identified by monitoring -> ***Longer TRS***
6 **Unplanned service break:** A: Disk space limitation of the database was not updated, when disk space was added -> ***Incident*** (Disc got full) -> B: Failure in monitoring agent -> A: no automatic alarm generated **-> *Longer TRS***
7 **Unsuccessful restoration of directories:** C: Configuration management -> B: Backup application did not support Windows version -> A: Long file names were not supported by OS but required by the applications -> ***Incident*** -> B: Access rights were not sufficient in troubleshooting activities -> ***Longer TRS***
8 **Problem with archive application**: C: Configuration management -> B: Components were not updated -> A: Old components caused performance degradation -> ***Incident***
9 **Unplanned service break:** C: Configuration management -> B: SW was not updated -> A: Old SW filled the disc -> ***Incident*** -> C: Event management -> B: No systematic monitoring policy -> A: Monitoring was not activated -> Incident is identified late -> ***Longer TRS***
10 **Network failure:** C: Capacity management -> B: Capacity of the redundant connections estimated incorrectly -> A: Router broken -> A: Overload in reserve connection -> ***Incident***
11 **Unplanned service break**: C: Capacity management -> B: Unexpectedly high amount of traffic -> A: Log files were filled -> ***Incident***
12 **Unplanned break in fax service**: C: No common change management with subcontractor -> B: Subcontractor changed the version of pdf file format -> A: Documents are not compatible with this version -> ***Incident***
13 **Network failure:** B: Broken fiber transmitter in redundant passive connection -> B: Lack of redundancy not communicated to the client -> A: Supervisory card failure in a switch on active connection -> ***Incident***
14 **Website down**: A: Network failure -> ***Incident*** -> B: Poor instructions -> A: Not all components were moved to another node in the first restoration attempt -> ***Longer TRS***
15 **Unplanned break in SAP service**: A: SW error (Application used all the memory) -> ***Incident*** -> B: Unclear text in the incident ticket -> A: Ticket routed to a wrong place -> ***Longer TRS*** **->** A: Poor documentation -> Not all the services were started -> ***Longer TRS***

IV. ANALYSIS

In the analysis stage, 15 IT service incidents were categorized according to the IT service incident model created in this study. The model was influenced by HFACS model, ITIL and the 215 incident reports used in this study. Regarding each incident, we analyzed how latent conditions had affected the formation of the incident, and how events during the incident affected restoration of service. The following five lessons learnt were identified in the analysis:

Lesson 1: *Latent, contributing factors should be investigated already in the original root cause analysis.* The quality of incident reports was poor for performing trend analysis. Only 27% of incident reports identified more than one root cause or contributing factor before or during the incident. Service improvement based on historical reports is challenging if the background of the incident is not opened. In order to identify service improvement opportunities one should go beyond the ordinary level of root cause "configuration error" or "network failure". This is in line with the findings of Saarelainen and Jäntti [6]. They also suggest, that in order to get more accurate results the principle of latent, contributing factors should be used already in root cause analysis phase.

Lesson 2: *The interface between event management and incident management needs to be clarified.* Event management focuses on managing automatic alerts created by IT infrastructure. In our case study, in four cases out of seven cases having incident within incident service restoration was delayed because of inadequate monitoring of events.

Lesson 3: *Configuration management.* There is a need for systematic configuration management. Four cases out of total 15 cases were affected by bugs and incompatibility caused by old software versions.

Lesson 4: *Duration of the incident.* Incident investigation should cover factors affecting the duration of incidents. Service downtime is one key parameter affecting the business impact of the incident and the SLA penalties. Until now the focus in incident investigation has been on the root cause, not on the downtime.

Lesson 5: *Role of tools, people, and processes.* The incident is often a mixture of conditions and events of all the above-mentioned elements added with external factors.

During our study, we identified some patterns (multiple levels of causality, "incident-within-incident") across the cases with causal relationships. In all of these cases there were at least one condition (level B in Figure 4) contributing to the direct cause (level A). Sometimes a poor process implementation (level C) was found with probable or apparent relationship to the condition.

 ISBN: 978-1-61208-451-0

In almost half of the cases, we identified a new phenomenon, namely, "incident-within-incident". This caused us to add time dimension in the model (Figure 5). This issue is addressed by ITIL indicating that change implementations may cause additional incidents. In our study we observed, that not only change implementations but also supporting tasks (incident detection, system repair, service restauration) during the incidents may trigger additional incidents.

In early phases in the analysis it was very clear, that HFACS model focusing mainly on human factors in incidents was not an adequate tool for our cases. Although previous studies and frameworks [28] have dealt with defect classification schemes, they have not provided classification that could be used successfully in the IT industry to manage a wide variety of IT service incidents. Additionally, the studies about distribution of top level root cause categories in Table II support this hypothesis. In our validation cases there were mixtures of process, technology and human related conditions and events in the very same causal link chain.

While RCA methods in general provides a process for conducting root cause analysis, 5-whys a thinking pattern, HAZOP brainstorming process, HFACS a human-centric error classification, our model aims at expanding error classification towards a more proactive and predictive model that would explain formation of incidents in an ITSM environment.

V. CONCLUSION

The research problem in this study was: How the incidents in ITSM operating environment could be modelled in order to aid proactive problem management, root cause analysis and continual service improvement. The research problem was divided into the following research questions:

Regarding the first research question (Can the idea in HFACS with latent factors be extended from human factors to technology and processes)? we found that extending the scope of top level incident root causes from human factors is a mandatory step. An incident often seems to be a mixture of all of these elements in different causal levels before and during the incident.

Regarding the second research question (Are there major differences in concept of incident in ITSM and in other industries?) we found that the IT service incident is already by definition different compared to the other industries. IT service incidents cover service failures as well as difficulties that service users experience while using IT services. An IT service incident has duration, which is a key component in the business impact of the incident.

Regarding the third research question (How these possible differences in the concept of incident should be taken into account in the model?) we found that in incident investigation more attention should be paid to events and conditions during the incident. Almost in half (7 cases of 15) of the incidents, we identified events or conditions that delayed restoring the service. As a general observation one can state, that business impact to the customer and SLA penalties by IT service provider are dependent on the duration of the incident.

There are, however, certain limitations in this study. The amount of sample cases was rather limited, only 15 cases. In future studies, we aim at conducting the study with a larger set of service incidents. The incident reports were prepared without knowing the incident model. The results would be more reliable if the incident investigator had studied systematically the latent conditions according the model. The case study results should not be used for statistical generalization but these have enabled us to extend the ITSM theory.

In the future work, adding probabilities to the model presented here may give predictive power to the model, especially if the probabilities and relationships are generated automatically or semi automatically from incident management records and configuration management database (CMDB). HFACS in the current format has limitations in ITSM environment, but an IT adaptation of HFACS may be useful related to human errors.

In the course of work, the poor quality of incident investigation and incident reports were observed. Lack of deeper analysis of contributing factors behind direct root causes gives poor starting point to proactive problem management and service improvement. This study has potential to increase incident awareness of persons working in related roles in ITSM. In order to effectively remedy the disease, one should know the mechanism.

The results in this study are useful for incident investigators and root cause analyst as well as to those involved in continual service improvement. This study gives tools to understand incidents more deeply and then fix the events and conditions increasing the probability of incidents.

ACKNOWLEDGMENT

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

 ISBN: 978-1-61208-451-0

REFERENCES

[1] Office of Government Commerce, ITIL Service Operation. United Kingdom: The Stationery Office, 2011.

[2] J. Reason, The contribution of latent human failures to the breakdown of complex systems. Philosophical Transactions of the Royal Society of London B: Biological Sciences 327(1241), 1990, pp. 475-484.

[3] K. Saarelainen and M. Jäntti, "Quality and human errors in IT service infrastructures - Human error based root causes of incidents and their categorization." in Innovations in Information Technology (IIT), 2015 11th International Conference on. 2015.

[4] D. A. Wiegmann, Human error analysis of commercial aviation accidents: Application of the human factors analysis and classification system (HFACS). Aviation, Space and Environmental Medicine 72(11) , 2001, p. 1006.

[5] K. Saarelainen and M. Jäntti, "Human errors in IT services - HFACS model in root cause categorization, " in International Scholarly and Scientific Research & Innovation, 2015, pp. 340-345.

[6] K. Saarelainen and M. Jäntti, "A case study on improvement of incident investigation process, " in System, Software & Service Process Improvement & Innovation 22nd European & Asian Conference, EuroSPI 2015, 2015 .

[7] S. A. Shappell and D. A. Wiegmann, Applying reason: The human factors analysis and classification system (HFACS). Human Factors and Aerospace Safety 1(1), 2001, pp. 59-86.

[8] R. Hanzu-Pazara, E. Barsan., and P. Arsenie, L. Chiotoriou and G. Raicu, "Reducing of maritime accidents caused by human factors using simulators in training process, " Journal of Maritime Research, vol. V, 2008, pp. 3-18.

[9] F. Aguirre, M. Sallak, W. Schon, and F. Belmonte, Application of evidential networks in quantitative analysis of railway accidents. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2013, pp. 1748006X12475044.

[10] L. Kohn T.., J. Corrigan, and M. S. Donaldson, to Err is Human : Building a Safer Health System. Washington, D.C.: National Academy Press, 2000.

[11] S. Hunziker, A. C. Johansson, F. Tschan, N. K. Semmer, L. Rock, M. D. Howell, and S. Marsch, Teamwork and leadership in cardiopulmonary resuscitation. J. Am. Coll. Cardiol. 57(24), 2011, pp. 2381-2388.

[12] R. Cintron, "Human Factors Analysis and Classification System Interrater Reliability for Biopharmaceutical Manufacturing Investigations", Walden Univesity, Maryland, USA, 2015.

[13] Managing Human Performance to Improve Nuclear Facility Operation 2013, IAEA Nuclear Energy Series, No NG-T-2.7International Atomic Energy Agency, Vienna, Austria, 2013.

[14] S. Ziedelis, M. Noel, and M. Strucic, Human based roots of failures in nuclear events investigations. Internationale Zeitschrift Fuer Kernenergie 58(10), 2012, pp. 596-601.

[15] K. S. N. Raju, Chemical Process Industry Safety, Tata McGraw-Hill Education, New Delhi, India, 2014.

[16] C. Karsberg and C. Skouloudi, "Annual incident reports 2014," European Union Agency for Network and Information Security (ENISA), 2015.

[17] L. Shwartz, D. Rosu, D. Loewenstern, M. J. Buco, S. Guo, R. Lavrado, M. Gupta, P. De, V. Madduri, and J. K. Singh, Quality of IT service delivery — analysis and framework for human error prevention. Presented at Service-Oriented Computing and Applications (SOCA), 2010 IEEE International Conference on, 2010, pp. 1-8.

[18] Ponemon Institute Research Report, "2013 cost of data center outages," Ponemon Institute, December 2013.

[19] K. Saarelainen and M. Jäntti, Creating an ITIL-based multidimensional incident analytics method: A case study. Presented at The Tenth International Conference on Systems ICONS, 2015, pp. 24-29.

[20] D. Hinz and H. Gewald, The next wave in IT infrastructure risk management: A causal modeling approach with bayesian belief networks. Presented at Emerging Trends and Challenges in Information Technology Management. 2006.

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

[22] E. Marcus and H. Stern. Blueprints for High Availability: Designing Resilient Distributed Systems, John Wiley \& Sons, Inc, New York, NY, USA 2000.

[23] Quorum, "Quorum disaster recovery report Q1 2013", 2013.

[24] Office of Government Commerce, IT Infrastructure Library - Service Delivery. London: The Stationery Office, 2001.

[25] Office of Government Commerce, IT Infrastructure Library - Service Support. London: The Stationery Office, 2001.

[26] Office of Government Commerce, ITIL Continual Service Improvement. United Kingdom: The Stationery Office, 2011.

[27] Office of Government Commerce, ITIL Service Design. United Kingdom: The Stationery Office, 2011.

[28] W. Florac, Software quality measurement: A framework for counting problems and defects. Software Engineering Institute, Carnegie Mellon University. Pittsburgh, PA. 1992.

[29] T. A. Klet, Hazop and Hazan: Identifying and Assessing Process Industry Hazards, Institution of Chemical Engineers, Rugby, UK, 1999.

[30] BSI: BS IEC 61882:2001: Hazard and Operability Studies (HAZOP studies). Application Guide, British Standards Institute, UK, 2001

[31] J. A. Mcdermid, M. Nicholson, and D. J. Pumfrey, "Experience with the application of HAZOP to computer-based systems." Presented at Compass '95: 10th Annual Conference on Computer Assurance, pp. 37-48, 1995.

 ISBN: 978-1-61208-451-0