# Evaluation of the Applicability of CM3: Emergency Problem Management within the Industry

Mira Kajko-Mattsson
ICT, KTH Royal Institute of Technology
Kista, Sweden
mekm2@kth.se

Joakim Snygg, Emil Hammargren
DSV, Stockholm University
Kista, Sweden
snygg@dsv.su.se, emil-ham@dsv.su.se

*Abstract*— **Software has become one of the main villains of many organizational problems, emergencies and crises. Despite this, there is only one process model defining how to manage emergency software problems. It is CM$^3$: Emergency Problem Management. In this paper, we evaluate the applicability of the *CM$^3$: Emergency Problem Management* model within five companies. Our results show that the model correctly manages the real-life emergency and crisis situations that are dependent on malfunctioning software. This evaluation shows that all the five companies have emergency processes that reflect CM$^3$ model's architecture, however, to different degrees. Additionally all the five companies have also designated roles that act as focal points of information and decision making during emergencies. Finally, only one company has identified the organizations and systems, which should be affected by the emergency process**

***Keywords-Problem management; operational levels; task force team; software maintenance.***

## I. INTRODUCTION

More and more of the emergencies and crises encountered today get generated due to malfunctioning software [1][6]. Many times, their underlying software problems may be of unpredictable and uncertain dimensions [16]. Being of high severity, they may threaten to harm the organizations' businesses and survival, their stakeholders, or the general public [8][10]. For this reason, software organizations must be well prepared for protecting themselves against all types of crises and emergencies by creating a well-defined emergency and crisis management process. It is only then they may guard themselves against all kinds of unexpected financial, political, legal, media and governmental impact and consequences. [7][9][11]

Emergency problem management is recognized as an important maintenance activity type by the International Software Engineering Standard - ISO/IEC 14764 [15]. Despite this, there are no process models providing guidelines for how to manage unexpected emergency and crisis problems. To our knowledge, there is only one model dedicated to software emergencies and crises today. It is *CM$^3$: Emergency Problem Management* [4][5]. CM$^3$ stands for *Corrective Maintenance Management Model*.

TABLE I. THE FIVE COMPANIES

| *Company* | *Nr of Employees* | *Nr of IT Employees* | *Domain* |
|---|---|---|---|
| SAS | > 12 000 | ≈ 150 | Aviation |
| Northern Finance | > 15 000 | > 100 | Finance |
| Bank and Loans | > 15 000 | ≈ 700 | Finance |
| Good Things | > 25 000 | ≈ 500 | Retail |
| Gladstone | ≈ 1 000 | ≈ 1 000 | Gaming |

*CM$^3$: Emergency Problem Management* was initially designed at *Scandinavian Airline Systems* (SAS) [4][5]. Hence, it reflected the status of SAS emergency process model. In this, paper, we study five industrial emergency processes with the purpose of evaluating *CM$^3$: Emergency Problem Management* and further extend it with more process elements. The five companies are SAS, *Northern Finance, Loans and Bank, Good Things and Gladstone.* Except for SAS, the companies have requested to stay anonymous. Hence, we use their fictitious names. The companies are briefly presented in Table I.

*Scandinavian Airlines* (SAS) is an aviation company member and cofounder of the Star Alliance. SAS is the ninth-largest airline in Europe.

*Northern Finance* operates within the financial sector. They are a worldwide finance company with offices from Asia to North America. However, their main business market is located in Europe. The company provides products and services in the financial sector such as trading, management and insurances.

*Bank & Loan ltd.* works within the financial sector and offers retail banking, asset management and financial services. They have offices in Asia, Europe, and North America, but their main business is in Scandinavia.

*Good Thing Sales* is one of the largest retail companies in Scandinavia with more than 1500 retail stores. Finally, *Gladstone Gamer* is one of the largest online gaming companies in the world. However, compared to the other companies in the study, this company is the youngest. Most of the employees are concerned with different aspects of IT.

The remainder of this paper is as follows. Section II presents our research method. Section III presents the extended version of *CM$^3$: Emergency Problem Management* Section IV describes how it matches the industrial emergency processes, and finally, Section V makes conclusions and suggestions for future work.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

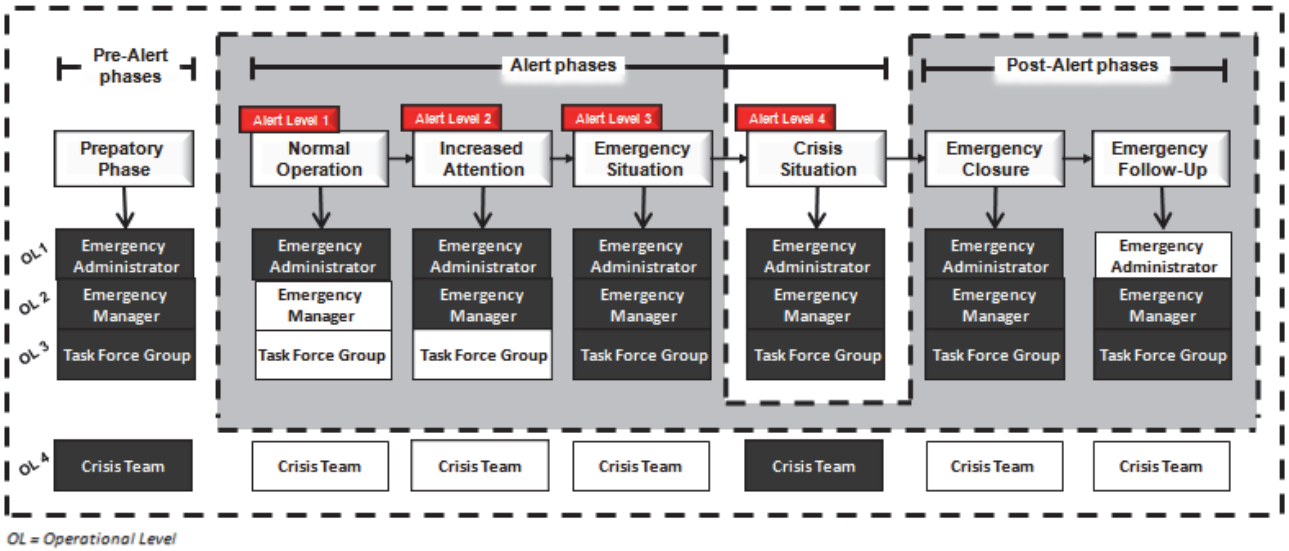


Figure 1. *CM³: Emergency Problem Management*

## II. METHOD

Our journey towards evaluating *CM³: Emergency Problem Management* consisted of many stages. Unfortunately, due to space restrictions, we cannot report on them all. Our reader may however, follow them by studying our former publications that describe the initial model design [4][5][12][13][14].

In general, our work consisted of four major stages: (1) design of the initial version of *CM³: Emergency Problem Management,* (2) evaluation of the model in the context of one financial company, (3) extension of the model, and finally, (4) model evaluation within five companies.

In the first stage, we developed the initial version of *CM³: Emergency Problem Management* within SAS [4][5]. This version is demarcated by the grey shaded area in Fig. 1. It is a better structured reflection of SAS emergency process model. Its main mission is to manage emergency software problems as encountered in SAS flight booking systems. When designing it, we had many unstructured and frequent interviews and discussions with SAS emergency process owner and emergency process executors. As a next step, we compared the model to an emergency process model within *Northern Finance* [12]. We chose this company mainly due to two reasons: (1) its application domain differed from the application domain at SAS and, therefore it provided a good platform for studying the applicability of the model in a different context, (2) emergencies in the financial sector were highly time dependent where the business stake was very high and where crisis had a substantial ripple effect on other sectors of the national economy [10].

During the study of *Northern Finance* emergency process, we interviewed *Information Officer*, *Incident Handler*, *Information Security Manager*, and *Emergency Escalation Partner* in a series of consecutive interviews using four different questionnaires. All of them were very comprehensive, semi-structured and open-ended. Altogether, they consisted of 300 main questions and additional 60 follow-up questions [13].

After having studied the emergency process at *Northern Finance,* we compared it to *CM³: Emergency Problem Management,* which we then extended with several process components. In Fig. 1, they constitute the components that are not part of the grey-shaded area. They mainly concern addition of *Pre-Alert* phase, *Operational Level 4* for managing crisis (see Fig. 1). When evaluating the model, we used a semi-structured and open-ended questionnaire consisting of 106 questions. On comparison with the questionnaires used in the second stage, the questionnaire in this stage was more of a comparative character whereas the former ones were more of an explorative type.

The comparison was made within five companies. Two of these were the companies that contributed to the creation and extension of *CM³: Emergency Problem Management*. These were SAS and *Northern Finance.* Three other organizations were new organizations. These were *Loans and Bank*, *Good Things*, and *Gladstone*.

Regarding the roles interviewed, at SAS and *Northern Finance,* we interviewed the same roles anew. Regarding the remaining organizations, we interviewed different roles. At *Loans & Bank,* we interviewed their *Production Group Leader*, a role in charge of task force teams. At *Good Things,* we interviewed their *Program Manager*, the head of IT security responsible for their incident management process and their contingency management. Finally, at *Gladstone,* we interviewed a shift leader, a role responsible for coordinating and resolving the emergency situations.

## III. CM³: EMERGENCY PROBLEM MANAGEMENT MODEL

*CM³: Emergency Problem Management* consists of six process components. They are (1) identification of the

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

TABLE II. EMERGENCY PROCESS ROLES

| Permanent Roles | | Temporaty Roles |
|---|---|---|
| ***Emergency Administrator***<br>•Focal point of contact during the entire emergency process.<br>• Accepts and controls all the emergency problem reports<br>• Take appropriate measures.<br>***Emergency Manager***<br>• Defines and improves emergency procedures<br>• Assists Task Force Team in managing problems<br>• Responsible for emergency management training<br>***Task Force Leader***<br>• Manages the resolution of the emergency problems.<br>• Leads the Task Force Team<br>***Task Force Team***:<br>• Responsible for the overall problem resolution, co-ordination of the emergency activities and tracking of the problem resolution.<br>• Ensures that appropriate actions are taken by all the parties involved in order to re-establish the normal operation with a minimum delay.<br>•Consists of two groups: permanent and temporary<br>***Permanent Task Force Group Members***<br>• Consists of key persons and IT management responsible for vital collaborating areas within the organisations involved. | ***Crisis Manager***<br>• Manages and Coordinates the Crisis Management Group<br>• Ensures that proper resources are available<br>***Crisis Management Group***<br>• Consists of business management roles and upper management<br>• Supports the Task Force Team with business sensitive knowledge and strategic decisions<br>• Consists of two groups: permanent and temporary<br>***Permanent Crisis Management Group Members***<br>• Consists of<br>•Crisis Group Chairman responsible for summoning and heading the Crisis Group meeting<br>• Crisis Communications responsible for organizing organization wide communication model.<br>• Crisis Security responsible for security issues mainly in the context of security-critical situations.<br>***ADDED! Crisis Security Manager***<br>• Monitors, handles and coordinates staff and all types of security issues<br>• Arranges proper physical protections<br>***ADDED! Crisis Communicator***<br>• Establishing communication routines<br>• Supplies information to the media, | ***Support Personnel***<br>• Consists of the support personnel on Support Line 1 and 2<br>• Reports on all the emergency problems to the Emergency Administrator.<br>***System Manager***<br>• Responsible for the system in which the problem was encountered.<br>***Developer/Maintainer***<br>• Responsible for changing the affected code.<br>***Temporary Task Force Group Members***<br>• Consists of System Managers, Support Personnel, Programmers, and other roles vital for resolving the emergency problem.<br>***Temporary Crisis Group Members***<br>•If needed, customer representatives and/or suppliers can partake in the Crisis Group meetings. |

Added stands for roles introduced to cm[3] after this study

organisations/departments/teams involved in the emergency process, (2) products to be managed by the emergency process, (3) roles involved in conducting the emergency activities, (4) the focal point of contact through which one communicates all emergency problems, (5) the emergency process and its phases, and (6) operational levels required for handling the emergency process. Although most of these constituents are present in any process model, their presence is extremely important within the emergency process. Inefficiencies in any of them may substantially affect the process results. In this section, we present each process component and the questions that have been asked for inquiring about their credibility and usefulness within the five companies studied. The questions are presented in Table III.

### *A. Identification of Organization*

Some software systems may be integrated with many systems that are many times evolved and maintained by several organisations. Hence, the first step when defining an emergency process should be to identify all the organisations involved in emergency situations.

To solve the problem efficiently, the collaborating companies must organize themselves and agree on and create a common emergency process model. For this reason, as indicated by Questions 18-29, we inquired about whether the companies studied involved other organizations in their respective emergency processes, and if so, whether they have agreed on a common emergency problem management process model.

### *B. Identification of the Product and Service Scope*

Not all products and services are critical to business or safety. Therefore, as a next step, the organisations should identify the products and services to be encompassed by the emergency process. These products and services are usually safety-critical and business-critical systems.

In addition to this, the organisations should define a pertinent scale for recording the severity levels of the problems encountered and determine which severity levels should be covered by the emergency process. If the process covers several severity levels, then one should define priorities for each level and specify in what way the management of the problems with different severity levels varies. Defining severity and priority should aid organizations in taking quick and appropriate measures preventing serious ripple effects and emergency escalations.

Using Questions 15-17 in Table III, we have inquired whether the organizations have identified the scope of products and services to be covered by the emergency process. We have also asked whether they have defined severity and priority values for these products and services.

### *C. Designation of Roles*

Designation of roles is especially important in emergency and crisis situations where conflicts of authorities, clashes over organizational domains, and organizational jurisdictional differences are common [4].

As shown in Table II, *CM[3]: Emergency Problem Management* identifies two groups of roles: *permanent* and *temporary*. By *permanent* roles, we mean the roles exclusively dedicated to manage the emergency situations. They are: *Emergency Administrator, Emergency Process Manager, Task Force Leader, Task Force Team,* and *Crisis Team*. By *temporary* roles, we mean the roles temporarily involved in the emergency process. They are *Support Personnel, System Users, System Managers, Temporary Task Force Group Members*, *Temporary Crisis Management Group Members* and other roles which are either responsible for the problematic system or are users of the system. Due to space restrictions, we cannot describe these roles in greater detail. We only list them and their main responsibilities in Table II. Interested readers are however most welcome to study them in [4][5][12][13][14].

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

When evaluating our model, we inquired about whether the companies studied used permanent and temporary roles within their emergency processes. We then went through *CM*[3]'s role list as presented in Table II and found out whether they were applicable within the organizations studied. At this step, we used Questions 73-82 in Table III.

### D. Point of Contact

During emergencies, information flow increases drastically. If not properly managed, it may cause loss of or it may delay the delivery of important information thus substantially intensifying the problem at hand and leading to a worsened situation [9][10]. For this reason, organizations should identify ways for how the emergency problems should be reported and communicated within the organization.

An emergency problem may be encountered in various ways by various roles such as end users, system managers, external organisations, or other. Each serious problem should be immediately reported to the relevant group which constitutes a focal point of contact. One should also specify the group's availability, both within and outside the office hours. In *CM*[3], such a point of contact is provided by *Operational Level 1* conducted by the *Emergency Administrator* role (see OL 1 in Fig. 1). Please observe that *Operational Levels* are not the same as *Support Line Levels* within industry. For more information about *Support Line Levels*, we welcome the reader to study [3].

Regarding the component *Point of Contact*, we used Questions 83-87 for inquiring whether the organizations studied have defined a focal point of contact for all their emergency problems and whether they have defined its availability.

### E. Process Phases

As outlined in the upper part of Fig. 1, the emergency process consists of three main phases. These are (1) *Pre-Alert Phase*, (2) *Alert Phases*, and (3) *Post-Alert Phases*. Below, we briefly describe them.

During the *Pre-Alert* phase – *Emergency Preparation*, the organizations prepare for various unforeseen emergency situations by defining or improving the emergency process, by regularly practicing it and by creating various actions and contingency plans [11]. During the *Alert* phase, the organizations attend to the encountered emergency problems. To effectively manage them, *CM*[3] distinguishes between four alert phases.

As soon as *Support Personnel* on *Support Line 1* gets a report on a serious problem, they are obliged to escalate it to the focal point of contact which is *Emergency Administrator* on *Operational Level 1* (see Fig. 1). At this moment, the problem and the process trades into the *Alert Level 1 – Normal Operation* phase. This phase only lasts for a predetermined period of time. Here, the *Emergency Administrator* collects all the information about the problem, monitors user reactions, evaluates problem severity and disseminates information to all the parties concerned.

After some predetermined period of time, the problem gets escalated to the next alert phase, *Alert Level 2 – Increased Attention*. It is now the *Emergency Manager* who becomes the owner of the problem. Together with one or several *System Managers*, he evaluates and implements possible workarounds, if any. The Emergency Manager acts as a focal point of decision.

After yet some predetermined period of time, the problem gets escalated to the *Alert Level 3 - Emergency Situation* phase. Now, the *Task Force Leader* is in charge of the emergency situation. His first action is to establish the *Task Force Team* who commonly tries to resolve the emergency problem. Finally, in cases when the problem threatens the organization's business and survival, the organization steps into the highest emergency level, which is *Alert Level 4 – Crisis Situation*. In this phase, the whole organization stands on toes including business managers and upper-level managers.

After the problem is resolved, the organization steps into the *Post-Alert* phases. Here, *CM*[3] distinguishes between two post-alert phases. These are *Post-Alert - Emergency Closure* and *Post-Alert – Emergency Follow-Up*. The *Post Emergency – Emergency Closure* phase is mainly executed by the *Task Force Leader* who writes a report on the problem and distributes it to all the parties concerned. The *Post-Alert – Emergency Follow-Up* phase, on the other hand, is conducted by the *Task Force Leader* who together with the *Emergency Manager* investigates the problem with the purpose of finding root causes underlying the problem. These causes provide an important feedback to process and product improvement.

When interviewing the companies, using Questions 30-52, we inquired whether they have defined pre-alert, alert and post-alert phases, what they do within these phases and what roles they involve.

### F. Operational Levels

The whole emergency process is conducted on four operational levels (see OLs in Fig. 1). The operational levels are only defined within the context of emergency and crisis management. They do not overlap with any other organizational levels, such as for instance, *Support Line* levels [3]. However, they may strongly co-operate with them.

The designation of operational levels is very important. The process execution is strongly dependent not only on the emergency phase the process is in but also on the operational level performing it. As summarized in Fig. 1, each group of roles has clearly defined responsibilities for each phase and operational level.

#### 1) Operational Level 1:

The *Operational Level* 1 is mainly conducted by the *Emergency Administrator*. It is involved in six process phases, the *Pre-Alert* phase, the four *Alert* phases and one *Post-Alert* phase – *Emergency Closure* (see Fig. 1). During the *Pre-Alert* phase, the individuals possessing the role of the *Emergency Administrator* exercise the emergency process and provide feedback for its improvement.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

TABLE III. EVALUATION QUESTIONAIRE

**General questions**
**Q1:** Name: Title: Department:
**Q2:** What is your job description and how long have you worked within the company and with similar tasks, concerning the emergency process?
**Q3:** Company name: Business field:
**Q4:** Nr. of employees… In total: Within the IT-department, Definitions and scope of the emergency process
**Q5:** Does your company determine the severity of incidents?
**Q6:** If yes, describe which
**Q7:** Does your company use priority codes on problems/incidents?
**Q8:** If yes, describe which
**Q9:** Does your company differentiate between software incidents and other incidents such as hardware and/or infrastructure related?
**Q10:** If yes, describe which
**Q11:** Does your company use a structured Crisis Management process at major disasters (such as fires etc)
**Q12:** If so can such processes be triggered by software incidents?
**Q13:** Can software incidents be of business critical magnitude?
**Q14:** Can software incidents be of a crisis magnitude?

**Product and Service scope**
**Q15**: Does your company have specific products, services or systems that especially initiate the emergency process?
**Q16:** If yes, describe if there are subsets and what is included in these subsets and why?
**Q17:** If yes, what is not included in these subsets and why?

**Organizational structure:**
**Q18:** Are there other organizations involved in the emergency problem process?
(External maintenance or development organizations as well as suppliers and important customer that may be affected)
**Q19:** If yes, describe which:
**Q20:** Have you agreed with these organizations on a common emergency problem management process?
**Q21:** Are there differences in the emergency problem process depending on time of day (as in or out of office hours, different contact areas)
**Q22:** If yes, describe which:
**Q23:** Do you use task forces on different levels during emergency situations?
**Q24:** If so what is it called?
**Q25:** Are there any other groups of interest in this context?
**Q26:** Can you be exposed to several emergency situations simultaneously?
**Q27:** If so, how is this coordinated?
**Q28:** Are parallel solutions suggestions developed?
**Q29:** If so; who decides on the solution to be implemented?

**Normal Operation phase**
**Q30:** Which activities are performed during emergency initiation in the Normal Operation Phase?
**Q31:** Which roles are active during emergency initiation in the Normal Operation Phase and what are their responsibilities?
**Q32:** Who is the problem owner during emergency initiation in the Normal Operation Phase and what are his/hers responsibilities?
**Q33:** Are there any time frames associated with the Normal Operation phase? e.g.
1) Time limits before it are allowed to alter the system? 2) Time limits within where information must be sent out? 3) Other time limits or regulations?

**Increased Attention Phase:**
**Q34:** Which activities are performed during the Increased Attention Phase?
**Q35:** Which roles are active during the Increased Attention Phase and what are their responsibilities?
**Q36:** Who is the problem owner during the Increased Attention Phase and what are his/hers responsibilities?
**Q37:** Are there any time frames associated with the Increased Attention phase?

**Emergency Situation Phase:**
**Q38:** Which activities are performed during the Emergency Situation Phase?
**Q39:** Which roles are active during the Emergency Situation Phase and what are their responsibilities?
**Q40:** Who is the problem owner during the Emergency Situation Phase and what are his/hers responsibilities?
**Q41:** Are there any time frames associated with the Emergency Situation phase?

**Emergency Closure Phase:**
**Q42:** Which activities are performed during the Emergency Closure Phase?
Q43: Which roles are active during the Emergency Closure Phase and what are their responsibilities?
**Q44:** Who is the problem owner during the Emergency Closure Phase and what are his/hers responsibilities?
**Q45:** Are there any time frames associated with the Emergency Closure phase?

**Emergency Follow-Up Phase:**
**Q46:** Which activities are performed during the Emergency Follow-Up Phase?
**Q47:** Which roles are active during the Emergency Follow-Up Phase and what are their responsibilities?
**Q48:** Who is the problem owner during the Emergency Follow-Up Phase and what are his/hers responsibilities?
**Q49:** Are there any time frames associated with the Emergency Closure phase?

**Preparations Phase:**
**Q50:** Which activities are performed during emergency preparations?
**Q51:** Which roles are active during the emergency preparations and what are their responsibilities?
**Q52:** Are there any time frames associated with the emergency preparations?

**Operational levels 1:**
**Q53:** Do you have operational levels?
**Q54:** How many Operational levels do you have?
**Q55:** What is their overall function?
**Q56:** Operational level 1:
**Q57:** Which are the responsibilities of this operational level?
**Q58:** What activities do occur at this level?
**Q59:** Which roles are active in this level?
**Q60:** What activities are these roles involved in during Normal Operation?

**Operational level 2:**
**Q61:** Which are the responsibilities of this operational level?
**Q62:** What activities do occur at this level?
**Q63:** Which roles are active in this level?
**Q64:** What activities are these roles involved in during Normal Operation?

**Operational level 3:**
**Q65:** Which are the responsibilities of this operational level?
**Q66:** What activities do occur at this level?
**Q67:** Which roles are active in this level?
**Q68:** What activities are these roles involved in during Normal Operation?

**Operational level 4:**
**Q69:** Which are the responsibilities of this operational level?
**Q70:** What activities do occur at this level?
**Q71:** Which roles are active in this level?
**Q72:** What activities are these roles involved in during Normal Operation?

**Roles:**
**Q73:** How many permanent roles are involved within the emergency process?
**Q74:** How many temporary roles are involved within the emergency process?
**Q75:** Does the following roles participate in the emergency process:
**Q76:** • System owner/manager? Where do they reside? Temporary/permanent? Activities during normal operation?
**Q77:** • System specialist? Where do they reside? Temporary/permanent? Activities during normal operation?
**Q78:** • Business manager? Where do they reside? Temporary/permanent? Activities during normal operation?
**Q79:** • Business specialists? Where do they reside? Temporary /permanent? Activities during normal operation?
**Q80:** • Support personnel? Where do they reside? Temporary/permanent? Activities during normal operation?
**Q81:** • Programmers? Where do they reside? Temporary/permanent? Activities during normal operation?
**Q82** • [Other roles]? Where do they reside? Temporary/permanent? Activities during normal operation?

**Information flow / Point of contacts**
**Q83:** Which focal point(s) are serious emergency problems reported to?
**Q84:** How is information disseminated?
**Q85:** Which are the target groups?
**Q86:** Are structured information channels set up (or already existent) during an emergency?
**Q87:** What are they?

**Measurement Methods (and analysis)**
**Q88:** Does your company measure the emergency process?
**Q89:** Exactly what do they measure?
**Q90:** What do you use it for?

**Preparations and process improvement**
**Q91:** Does your company practice to resolve emergency incidents (aka scenario-based training)?
**Q92:** Does your company perform process reviews concerning emergencies? (e.g.: Review Document Sittings.)
**Q93:** Does your company have technical oriented training activities concerning emergencies?
(e.g. contingency testing where the primary site is taken down and a secondary are used instead)
**Q94:** Does your company use any other form of training concerning emergencies?
**Q95:** Are there any analyses of the root causes of the emergency problem? (i.e. site-specific notes)
**Q96:** Is there any feedback to such analysis?
**Q97:** If yes, describe who
**Q98:** Are processes and the methods of working evaluated or analyzed?
**Q99:** If yes, describe which
**Q100:** Are there any couplings back to the process from such analysis?
(e.g. lessons learned)
**Q101:** If yes, describe which

**Artifacts**
**Q102:** Does your company use artifacts for providing and managing the execution of the emergency process workflows? (e.g. checklists and case management tools to support workflows according to processes)
**Q103:** Does your company use artifacts for operational management of a certain domain or aspect of one?
(e.g. Configuration Management databases, monitoring system, diagnosis tools).
**Q104:** Does your company use artifacts for contingency and recovery of business critical system?
(e.g. double systems to reduce impact and RAID and Back-Up solutions to improve system recovery)
**Q105:** Do these tools support the company´s working processes?
(e g adjusted for ITIL)

**Extra:**
**Q106:** Are there any other qualitative measurements used? (show the paper with qualitative crisis measures)

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4

The responsibilities of the *Emergency Administrator* role vary during the *Alert* phases. In the first *Alert* phase, they own the problem. Here, they confirm the problem, establish an internal emergency log, record relevant information in it, and distribute it to all the parties concerned. The information basically specifies the problem, its occurrence, its cause, expected impact, and other relevant data.

During the remaining *Alert* phases, the *Emergency Administrator* continues administrating the problem, and informing all the parties concerned about the status of the problem. However, he no longer owns the problem. Finally, in the *Post-Alert* phases, the Emergency *Administrator* records all the problem information and informs all the parties concerned about its resolution.

The *Operational Level 2* is conducted by mainly two roles: *Emergency Manager* and *System Manager(s)*. The *Emergency Manager* has many responsibilities. One of them is to support the *Emergency Administrator* in all the emergency situations. He also coordinates workarounds received from the *System Manager(s)*. The responsibility of the *System Manager(s)*, on the other hand, is (1) to be available to the *Emergency Administrator* and the *Emergency Manager*, (2) to provide them with the necessary information and (3) to attend to the tasks requested by them.

*2) Operational Level 2*

The *Emergency Manager* and *System Manager(s)* start having duties on Alert *Level 2*. During the Increased *Attention* phase, the *Emergency Manager* becomes the problem owner. However, he is continuously supported by the *Emergency Administrator* with various administrative tasks. He also involves *System Manager(s)* responsible for the systems or system parts that got affected by the problem, creates workarounds in cooperation with the *System Manager(s),* and distributes information to the relevant management.

During the remaining alert phases, the *Emergency Manager* gets rid of his problem ownership. He now supports the *Task Force Team* with various tasks.

During the *Post-Alert* phases, the *Emergency Manager* continues to support the *Task Force Team*. He also evaluates the emergency process, makes suggestions for improving it and realizes them, if deemed relevant and necessary.

*3) Operational Level 3*

The *Operational Level 3* is mainly conducted by the *Task Force Leader* and *Task Force Team*. The roles and number of participants in the team varies depending on problem type. If, for instance, three systems are involved, then it automatically implies that three *System Managers* and their teams are involved.

The responsibilities of the *Task Force Leader* role start during the *Alert 3* phase. The *Task Force Leader* establishes a *Task Force Team* and ensures that the team is in place. Afterwards, the course of actions varies depending on the problem. However, the *Task Force Leader* acts as a focal point of entry for all the management contacts, ensures that all parties concerned are informed, leads the *Task Force Team*, co-ordinates the emergency activities, initiates activities leading to the reduction of user impact, makes sure that the initiated activities are taken according to the defined procedures, and initiates workaround's or other problem solutions.

After the problem has been resolved, the *Task Force Leader* produces a report containing (1) time when the problem first occurred, (2) description of what happened and why, (3) description of the impact, (4) measures taken to limit the impact, (5) time stamp when the problem got resolved, (6) description of the measures taken in order to resolve the problem, (7) status of the emergency procedures used, (8) action list for changes to the emergency procedures, and (9) suggestions for how to prevent similar situations.

During the *Post-Emergency – Follow-Up* phase, the *Task Force Leader* makes additional investigations of the problem and its causes together with the *Emergency Manager*. If the emergency problem is followed by a planned and scheduled problem resolution, then they should monitor its resolution.

In this phase, the *Task Force Leader* has regular meetings with the relevant roles and organisations or departments during which they follow up all problems of high severity. The goal is to find ways to avoid future emergency situations. Hence, a vital task of this phase is to specify measures to prevent the problems from occurring. These measures should be recorded and delivered to the process improvement process.

*4) Operational Level 4*

The *Operational Level 4* is only active in clear crisis situations. Crisis is an extraordinary situation that needs involvement from top management whose responsibility is to evaluate business threats and make important decisions on finances, personnel and other resources. It is led by *Crisis Management Group* and it is supported by *Task Force Team*. The roles and number of its participants varies depending on the crisis type.

During the interviews, using Questions 53-72, we inquired whether the organizations studied have defined their correspondences to *CM³ Operational Levels*, what roles are involved in these levels and what their responsibilities are.

## IV. EVALUATION OF THE CM³: EMERGENCY PROBLEM MANAGEMENT MODEL

In this section, we present the evaluation results of *CM³: Emergency Problem Management* within the companies studied. When doing it, we follow the order of process components as defined in Section III.

### *A. Identification of Organisations*

All the five companies have defined an emergency problem management process. However, only four of them need to involve external organizations in their emergency situations. All four of them have agreed on an emergency problem management process model to be commonly run by all the parties involved.

### *B. Identification of the Product and Service Scope*

Only one organization identifies products and services that undergo an emergency process. It is SAS. SAS does it indirectly by classifying systems according to how soon they should be recovered. In the remaining companies, the products and services are too tightly coupled to one another

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

implying that a problem in one system might lead to a substantial ripple effect within the whole organization or even several organizations. Hence, all the products and services undergo an emergency process. The process gets enacted on the basis of an emergency case, its context, severity value and a number of the affected functions or customers.

All the organizations studied have defined severity and priority (urgency) values for their products and services. An example of how one organization formally calculates severity levels is illustrated in [12]. One of the organizations studied, however, does not have any formal definition of severity and priority. Being within online gaming industry, their severity is informally estimated by counting the number of the affected users.

Except for SAS, when enacting their emergency processes, the organizations mainly follow the urgency value and the number of the reported incidents for the emergency problem or the problem severity.

### C. Emergency Management Roles

All the companies studied have defined both permanent and temporary roles. Regarding the permanent roles, all the companies have the equivalences of *Emergency Administrator, Emergency Manager* and *Task Force Leader.* However, their naming strongly differs. The role of *Emergency Administrator* is, for instance, mainly conducted by support personnel in two organizations. Other role names corresponding to *Emergency Administrator* are *Operation Manager* and *Operator* at a control department.

Regarding the role of *Emergency Manager,* we have found out that all the companies use the *Emergency Manager* role to different degrees; from providing assistance concerning problem escalation to being very active in supporting the emergency resolution process and to providing quality assurance to the *Task Force Leader*.

Regarding the role of *Task Force Leader*, all the five companies use this role as a single point of decision in the *Emergency Situation* phase. The role is primarily responsible for getting the impacted systems' functionality up and running and he has the authority to assign resources, if needed.

Four out of five organizations involve *Crisis Management Group*. The group is a meeting board responsible for the overall IT and business coordination and management. It deals with all crises related issues. It decides when to declare disaster and when to start acting according to the contingency plans.

Finally, our study has revealed the need for two additional however very important roles, *Crisis Communicator* and *Crisis Security Manager*. These roles are implemented in four of the five organizations studied. The responsibility of the *Crisis Communicator* is to manage communication on emergency problems between the organization and the public. The responsibility of the *Crisis Security Manager*, on the other hand, is to monitor, handle and coordinate staff and all types of security related issues, and to arrange proper protection

All the companies studied use temporary roles in their emergency processes, such as *Support Personnel, System Manager* and *Developer / Maintainer*. Regarding *Support Personnel*, they all have its corresponding role supporting the customers in their daily operation. It is this role that may overlap or may be merged with the role of the *Emergency Administrator*.

### D. Focal Point of Contact

All the companies studied have an appointed role, or a group of roles, that act as a focal point of contact for all the emergencies. The roles involved vary. At SAS, for instance, *Operational Level 1* corresponds to the first point of contact during office hours. After a serious problem gets reported to *Support Line 1* [3], it automatically gets escalated to *Operational Level 1*. Outside office hours, however, the problem gets reported to *Support Line 1* belonging to an outsourced organization. This organization, in turn, contacts *Operational Level 1* in cases when they deem that the reported problem is serious. Regarding the remaining organizations, the *Emergency Operator* at *Operational Level 1* corresponds to *Support Line 1* being on duty around the clock [3].

### E. Process Phases

Due to the fact that the organizations studied have not had any emergency standard to follow, they have defined their emergency processes on their own. For this reason, their models differ. Still, however, we could identify many common parts.

#### 1) Pre-Alert Phase

All the organizations studied prepare themselves for various emergency and crisis situations. Hence, they have a phase corresponding to *CM*$^3$*'s Pre-Alert Emergency Preparation* phase. During this phase, they mainly review the emergency process and its supporting documents. Four out of five companies even conduct sporadic scenario-based training several times a year.

Different roles are responsible for the pre-alert emergency process within the organizations studied. They are *Contingency Manager* and various other industrial correspondences to *CM*$^3$ *Emergency Manager*.

#### 2) Alert Phases

Reporting on serious problems/incidents to *Support Line 1* enacts the first emergency phase, *Alert Level 1 – Normal Situation,* in four of the organizations studied. At SAS, however, the problems get immediately escalated from *Support Line 1* to *Operational Level 1*, which, in turn, initiates the emergency process.

As mentioned in Section 4.3, only SAS has explicitly identified the *Emergency Administrator* role. In the other companies, the role of the *Emergency Administrator* is performed by other roles, such as support personnel or other administrative or technical roles.

In four out of five companies, the problem gets escalated to the next phase, the *Alert Level 2 – Increased Attention* phase. In these companies, the problem is now owned by the role corresponding to the *Emergency Manager* who tries to find a workaround and makes preparations for the next alert

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

phase. In the fifth company, *Good Things*, severe problems are directly escalated from *Support Line 1* to their correspondence to *CM*[3]'s *Task Force Team* which they call *24/7 Group.*

All the companies studied have a phase corresponding to the *Emergency Situation* phase during which the *Task Force Leader* coordinates the resolution process. In three out of five companies, the first task of this role is to form a *Task Force Team.* In the other two companies, the *Task Force Leader* assigns the emergency task to one or several departments.

Regarding the *Alert Level 4 – Crisis Situation* phase, it is practiced in four out of five companies studied. Here, all business related decisions are made by the *Crisis Management Group*. This phase is triggered only in very critical business cases. The fifth company, which is a relatively young company, does not practice crisis management process yet.

Our study has revealed that the involvement of *Crisis Management Group* is immensely important in making critical decisions. Their decisions may override the decisions of *Task Force Group*, even in cases when IT solutions are more optimal than the business ones. Usually, this happens when safety or business gains are more prioritized than anything else. Scenario describing such cases is provided in [12][13].

Regarding the CM[3]'s suggestion for determining time period for each alert phase, only SAS does so. The other companies continuously monitor the problem during the early alert phases and escalate it to higher alert phases only if the problem and its impact intensify.

*3) Post-Alert Phases*

Only two companies have explicitly defined a correspondence to the *CM*[3] *Post-Alert Emergency Closure* phase, which is conducted by the *Task Force Leader*. Just as in CM[3], the *Task Force Leader* is responsible for the follow up of the emergency cases. In the other three companies, the ownership of this phase is assigned to an *Emergency Manager* or *Root Cause Analyst.*

Irrespective of who owns the phase, all the companies studied finalize their emergency processes by having a meeting during which the problem is officially closed. In addition, three of them write and disseminate a final report on the problem and its solution.

Regarding the *Emergency Follow-up* phase, in four companies, this step is conducted by the *Task Force Leader* alone or in collaboration with other roles such as *Emergency Manager* or *Task Force Team Members*. However, the tasks defined for this phase are not always realized. Both root cause analysis and process improvement may be conducted on an ad hoc basis or they may not be conducted at all.

*4) Operational Levels*

Only one company has explicitly defined the operational levels as defined in CM[3]. It is SAS. Regarding the remaining companies, they have done it implicitly. They follow similar levels; however, they do not call them operational levels.

All but one organization have correspondences to four operational levels. Regarding the fifth organization, as has already been mentioned, this organization is young. It has not yet managed to implement the *Crisis Situation* phase. Hence, it does not have any correspondence to *Operational Level 4*.

The scenario of defining operational levels looks as follows in the organizations studied. At their correspondences to *Operational Level 1*, support personnel, customer service representatives, or *Emergency Administrator* are the main actors. They are problem owners in the initial emergency phases, which they then hand over to the roles on the next operational level.

The main actors at the industrial correspondences to *Operational Level 2* are the *IT Support Coordinator*, *General Escalation Point* (GEP), *Emergency Escalation Partner* and *Emergency Manager* (at SAS). All these roles have the responsibilities corresponding to those of CM[3]'s *Emergency Manager*

All the organizations studied involve correspondences to *CM*[3]'s *Task Force Teams* on *Operational Level 3*. Three of them actually use the same name. In one company *Task Force Leader* was called *Incident Handler*. Only two companies use different names such as *24/7 Group* and *Shift Leader*.

Regarding the industrial correspondences to *Operational Level 4*, as mentioned earlier, only four organizations have implemented it in their process models. They use the same role names as in CM[3]. One company, however, calls the CM[3]'s correspondence to *Crisis Manager* as *Critical Situation Manager (CSM).*

## V. CONCLUSION

Due to the fact that the software community lacks a common emergency maintenance process model, many organizations have defined their own local emergency process models. In this paper, we have studied five industrial emergency maintenance processes with the purpose of evaluating the applicability of *CM*[3]*: Emergency Problem Management* within five companies. The companies running these processes differ in size, industrial domains and process maturity. Despite this, with the use of an open-ended questionnaire and *CM*[3]*: Emergency Problem Management*, we could identify their common parts and directly map them on *CM*[3]*: Emergency Problem Management.* Here, the *CM*[3] model has acted both as a helpful tool for evaluating industrial emergency process models as well as an excellent tool for evaluating itself and its structure. It has helped us to find many commonalities on how to meet emergency situations and it has helped us to identify some minor differences among the processes studied. Below, we briefly list our findings, comment on them and comment on how they contributed to enhance the quality of *CM*[3]*: Emergency Problem Management.*

All the organizations studied have defined an emergency problem management process to be either used locally for managing their internal emergencies or as a common process to be used together with their partners. Hence, they constitute an appropriate forum for evaluating *CM*[3]*: Emergency Problem Management*.

- Not all the organizations identify the scope of their product and service portfolios that might be subdue

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

to emergency problem management. A strong coupling among the systems and magnitude of the potential ripple effect makes four out of five organizations be very sensitive to all types of emergency problems in all their systems. Hence, we conclude that the design of products and services in these companies is not amenable for defining and enacting the emergency process. The organizations must be on a constant alert about all types of incidents that are encountered in all their products and services. This is not an effective way of managing organizational resources. As a remedy, we suggest that the organizations studied make effort in decoupling their critical systems so that the emergency process may be isolated to a specific system or even system part.

- Despite process differences in the organizations studied, all the organizations have defined software emergency process models that consist of pre-alert, alert and post-alert phases and that include activities and responsibilities that are organized in a similar manner as CM$^3$'s operational levels. [4][5][12][14] However, the number and names of their alert phases may vary. The pre-alert and alert activities are actively conducted whereas the post-alert activities such as collecting lessons learned were sparse, and were usually only conducted in an ad hoc manner. While studying the stages, we realized that the pre-alert stage of CM$^3$: Emergency Problem Management needs to be explored more in depth.
- Two of the companies have defined an additional emergency operational level, the level dealing with crisis management. The other companies had a crisis management processes, but this process was not aligned with the emergency process. Crisis management is used only in cases when a software problem jeopardizes human life and/or company's financial position or survival. For this reason, we have enhanced *CM$^3$: Emergency Problem Management* with a crisis phase, *Crisis Situation*, on top of the emergency phase and added an additional operational level, Operational Level 4, the level only dealing with crisis management.
- Involving crisis management is more common in financial and aviation sectors than in other sectors. Still, however, the organizations studied have not been able to optimally integrate crisis management process with software problem management process. By not having an integrated crisis management process, a set of issues is raised when the two processes work side by side: (1) how to deal with single point of decision and (2) how to deal with a focal point of information during high priority emergency situations. At the moment of writing this paper, SAS is in the process of connecting the emergency incident process with the business crisis management process.
- All of the companies have implicitly defined actions to meet a software emergency situation, and these actions were conducted by a number of predefined emergency roles. These roles are either temporary or permanent emergency maintenance roles. However, four out of five have a clearly defined crisis management group. In our study, we have identified new roles such as *Crisis Management Group, Crisis Manager, Crisis Communicator*, and *Crisis Security Manager*. All these roles have been added to the CM$^3$ model due to its extension with an additional alert phase, *Crisis Situation*, and an additional operational level, *Operational Level 4*.
- All the companies had also identified focal points for the information flow to and from the emergency team. In all cases, it is support personnel that accepts emergency problem reports and either continues managing them or hands them over to *CM$^3$*'s correspondence to *Emergency Administrator.*
- Regarding *CM$^3$*'s suggestion for determining time period for each alert phase, only SAS does so. They do so because they have specified rules for how soon their systems should be up and running. The other companies continuously monitor the problem during the early alert phases and escalate it to higher alert phases only if the problems and their impact intensify. This is because not all problems are directly recognized as very serious and urgent. To make our model adaptable to this new finding, we change the escalation rules from only time-dependent to both time and impact dependent.
- Most of the companies conduct post-alert phases mainly on an ad hoc basis. Reasons are many. One of them is the fact that the organizations do not designate enough resources for this important phase. Another reason is the fact that the report on the emergency problem and measures is disseminated too late. Its receivers lose interest in taking any measures whatsoever due to new problems that they have to deal with instead.
- Only one company has explicitly defined operational levels. The other companies have implemented operational levels implicitly by defining operational responsibilities and tasks and making sure that they do not overlap across the roles involved in emergencies.

Our evaluation study was huge. Hence, we could not present all our findings. We only had to concentrate on the most important ones. Using them as a basis, we may claim that *CM$^3$: Emergency Problem Management* is applicable within the industry. There are many commonalities between *CM$^3$: Emergency Problem Management* and the industrial emergency process models studied. We believe that our work on CM$^3$: Emergency Problem Management shows evidence for the presence of software emergency processes and the need for a standard that can aid practitioners in setting up and evaluating their local processes.

Our work on CM$^3$ is still in an early stage. Due to the fact that the emergency process is very comprehensive and complex, more studies are needed to fully evaluate the

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 

model. In brief, the following research action points need to be considered:

- The pre-alert phase needs to be further investigated. Two actions are proposed: 1) to survey training and education efforts, and 2) to explore how lessons learned from previous incidents can be used as feedback into the emergency maintenance process.
- Evaluate *CM³: Emergency Problem Management* within other industrial sectors such as, for instance, health care and e-government. Due to their nature, potential emergencies can be disastrous in these fields.
- Coupling *CM³: Emergency Problem Managemen*t with crisis management. Several issues are of interest such as mapping a single point of technical decisions from the emergency process onto a single point of organizational decisions from the crisis management and vice versa and define enterprise-wide agreements on when to declare a crisis situation.
- Integrate *CM³: Emergency Problem Management* with the development phases of the software lifecycle, identify how they impact each other and clarify borders between software emergency maintenance and other processes such as risk management, scheduled problem management and the like.

Despite many action points required for evaluating the model, we strongly believe that *CM³: Emergency Problem Management* already provides solid guidance for software organizations in their attempts to define and improve their emergency software maintenance process models.

## REFERENCES


[1] A. Brown and D. Patterson, "Embracing failure: A case for Recovery-Oriented Computing (ROC)". In Proceedings of the 2001 High Performance Transaction Processing Symposium, 2001, pp. 3-8.

[2] M. Kajko-Mattsson, “Motivating the Corrective Maintenance Maturity Model (CM3)”, In Proceedings of the Seventh IEEE International Conference on Engineering of Complex Computer Systems, IEEE, 2001, pp. 112-117.

[3] M. Kajko-Mattsson, Corrective Maintenance Maturity Model: Problem Management, PhD thesis, ISBN Nr 91-7265-311-6, ISSN 1101-8526, ISRN SU-KTH/DSV/R--01/15, Department of Computer and Systems Sciences (DSV), Stockholm University and Royal Institute of Technology (KTH), 2001.

[4] M. Kajko-Mattsson, C. Nielsen, P. Winther, B. Vang and A. Petersen, "An Outline of CM3: Emergency Problem Management," In Proceedings of EUROMICRO Conference on Software Engineering and Advanced Applications, 2005, pp. 292-303.

[5] M. Kajko-Mattsson, C. Nielsen, P. Winther, B. Vang and A. Petersen, 2006. "Eliciting CM3: Emergency Problem Management at Scandinavian Airline Systems", Journal of Research and Practice in Information Technology, 2006, vol. 38, no. 4, pp. 303-316.

[6] D. L. Parnas, A. J. van Schouwen and S. P. Kwan, "Evaluation of Safety-Critical Software" Communications of the ACM, vol. 33, no. 6, pp. 636-648, June 1990, doi:10.1145/78973.78974

[7] T.C. Pauchant, and R. Douville, 1993. "Recent research in Crisis Management: a study of 24 authors’ publications from 1986 to 1991", Organization & Environment, vol. 7, no. 1, pp. 43-66, Jan 1993, doi: 10.1177/108602669300700104.

[8] C. M. Pearson and J. A. Clair, "Reframing Crisis Management", Academy of Management Review, vol. 23, no. 4, pp. 59-76. Academy of Management, 1998, doi: 10.5465/AMR.1998.192960.

[9] E.L. Quarantelli, "Disaster Crisis Management: A summary of research findings", Journal of Management studies, vol. 25, no. 4, pp. 373-384, 1988. ISSN: 0022-2380

[10] A. Reilly, "Preparing for the worst: the process of effective crisis management" in Organization Environment, vol. 7, no. 2, pp. 115-143, Jan 1993, doi:10.1177/108602669300700204.

[11] D. Smith, "Beyond contingency planning: towards a model of crisis management", Industrial Crisis Quarterly, vol. 4, pp. 263-275, Jan 1990, doi:10.1177/108602669000400402.

[12] J. Snygg, M. Kajko-Mattsson, and E. Hammargren, Comparing two software emergency process models. In: 2012 International Conference on Software and System Process (ICSSP). Zürich: IEEE Conference Publications, 2012 pp.150-159

[13] J. Snygg and E. Hammargren, 2010. “Handling Crisis Within CM3: Emergency Management Process” master thesis, Dept. of Computer and Systems Sciences., Stockholm University/Royal institute of Technology., 2010.

[14] M. Kajko-Mattsson, J. Snygg, and E. Hammargren, CM3: Emergency problem management - A scenario-based evaluation. In: Information Science and Digital Content Technology (ICIDT), 2012 8th International Conference on Jeju Island, Korea (South): IEEE, 2012, pp.379-386

[15] ISO/IEC 14764., (IEEE, std 14764-2006). Software Engineering-Software Life Cycle Process-Maintenance, The Institute of Electrical and Electronics Engineers, Inc., 2006.

[16] M. Kajko-Mattsson, Common Concept Apparatus within Corrective Software Maintenance, Proceedings, International Conference on Software Maintenance, IEEE Computer Society Press: Los Alamitos, CA, Sep 1999, ISBN: 0-7695-0016-1, pp. 287-297.


Copyright (c) IARIA, 2014. ISBN: 978-1-61208-367-4 