UDK 004.41:005
Original scientific paper

# PROACTIVE APPROACH TO THE INCIDENT AND PROBLEM MANAGEMENT IN COMMUNICATION NETWORKS

**[1]Vjeran Strahonja, [2]Kristijan Saletović**
[1]University of Zagreb, Faculty of Organization and Informatics, Varaždin, Croatia
*vjeran.strahonja@foi.hr*
[2]COM CS S IN, Siemens d. d., Zagreb, Croatia
*kristian.saletovic@siemens.com*

**Abstract:** *Proactive approach to communication network maintenance has the capability of enhancing the integrity and reliability of communication networks, as well as of reducing maintenance costs and overall number of incidents. This paper presents approaches to problem and incident prevention with the help of root-cause analysis, aligning that with the goal to foresee software performance. Implementation of proactive approach requires recognition of enterprise's current level of maintenance, better insights into available approaches and tools, as well as their comparison, interoperability, integration and further development. The approach we are proposing and elaborating in this paper lies on the construction of a metamodel of the problem management of information technology, particularly the proactive problem management. The metamodel is derived from the original ITIL specification and presented in an object-oriented fashion by using structure (class) diagrams conform to UML notation. Based on current research, appropriate metrics based on the concept of Key Performance Indicators is suggested.*

**Keywords:** *Proactive maintenance, Problem management, Metamodeling, UML based metamodel.*

## 1. INTRODUCTION

Maintenance, being the end phase of a project, is dynamically developing along with the demands of the modern market and has therefore been recognized as an important activity within program engineering [11]. Safe and continuous performance of the program system is one of the most important links in the modern business. Detecting, isolating and solving problems in their earliest phase reduces greatly the danger of possible outages of certain parts of the system or of the entire system and in that way directly influences business [21].

Effective maintenance management is critical to the operation of communication networks. Taking into consideration various concepts of program systems, managers may plan and undertake network management and maintenance activities proactively or reactively. Reactive approach initiates maintenance activities after some failure or problem occurs. This approach is typical for traditional industries where cost cutting has become the highest priority. Due to current market conditions, communication networks management managers take preventive measures before crises occur. As the name implies, proactive approach uses well-planned and executed preventive measures to impede failures and shutdowns. This is a way to reduce lost revenues and overall downtime costs.

## 2. CURRENT APPROACHES TO PREVENTIVE MAINTENANCE

Part of the maintenance organization efforts should be vectored toward the use of predictive tools to help in monitoring the "health" of the communication equipment. For this purpose NOC (Network Operations Centre) should make full use of management systems capabilities imbedded in the communications and network management protocols [7]. Usage of historical performance data, collected with monitoring activities, can be applied for determining performance trend, scheduling future tasks in maintenance and predicting potential degradation of services. It is generally recommended [10] that historical records should be retained for at least 12 months to allow the identification of persistent degraded and faulty conditions.

According to [9] well-organized preventive maintenance process should consists of (i) supervision process for anomalies (short period), (ii) the defect supervisory process (medium period) and (iii) the malfunction supervisory process (long period). It can be based on statistical or analytical identification methods; nevertheless it should cover all three concurrent levels of supervision.

Early detection of threshold violation in system performance is very useful in avoiding future problems and in planning proactive maintenance activities. This can be done with system performance logs analysis, gathering of specific performance related data, comparison of gathered and current data, fault monitoring, detection and notification – all that for the ultimate goal to predict and to be prepared for applying proactive measures. Recent trend in preventive maintenance of telecommunication systems is usage of AI systems that gather information, have learning capabilities and use research methods. Operating system recovery described in [5] presents proactive approach to operating system stability. Operating systems that need to be available 24 hours 7 days a week require *fine-grain proactive recovery* of operating system components. In that way modules are restarted periodically to keep their status clean of memory leaking, data corruption, storage space fragmentation or infinite loops. Many studies have reported phenomenon of "Software aging" that describes the state of software performance that degrades with time. For this purpose "Software rejuvenation" is proactive technique described in [22] aimed at preventing unexpected or unplanned outages due to aging. The basic idea is to stop the running software, clean its internal state and restart it. Proactive approach in TCP/IP networks functions by constantly testing vulnerabilities and exposures to threats (security breaches, digital attacks and spam). Those tests are then assessed and prioritized according to those vulnerabilities and exposures. All IP devices attached to the network are periodically or continuously scanned and profiled for changes, violation of policy, and vulnerabilities and exposures. Analytics are applied so that the administrators and business owners are presented with actionable intelligence relative to the risk to their business. The defect is then corrected, before security can be breached [12].

Gathering useful performance data can be done in different ways and it is up to engineers and other specialists to find appropriate solution for it. A few trends are present [21]:

- Usage of remote monitoring for alarms, thresholds and other important events,
- Usage of event management routines,
- Usage of network simulation tools to optimize predictive maintenance decisions in real time.

## 3. MAINTENANCE BEST PRACTICES

Developing business processes from scratch can result in increased costs without noticeable improvement in comparison to proven industry standards and practices, therefore, many organizations are looking for suitable experience for their typical line of business.

Best maintenance practices in communication networks management are benchmarking standards that, if carefully implemented, will enhance the integrity, reliability and maintenance costs of communication networks. Term “best practice” can mean different things to different people, and because of that there is general consensus that this term involves tracking the practices of other companies in order to compile a list of benchmarking standards that constitute stretched goals. According to Kamoun [7] well-articulated best practices should be:

- Precise and measurable; if this requirement is not satisfied companies will lack the possibility to asses their progress,
- Challenging, yet realistic and if possible provable,
- With defined deadlines.

The British Office of Government Commerce (OGC) and the IT Service Management Forum (itSMF) provide a collection of best practices for IT processes in the area of IT service management which is called ITIL (IT Information Library) [6, 16, 17]. The service management is described by 11 modules which are grouped into Service Support set (provider internal processes) and Service Delivery set (processes at the customer-provider interface). Each module describes processes, functions, roles, and responsibilities, as well as necessary databases and interfaces. In general, ITIL describes contents, processes, and aims at a high abstraction level and contains no information about management architectures and tools. In ITIL Fault Management is divided into Incident Management process and Problem Management process [3]. This paper is oriented to proactive approach of Incident and Problem Management process and therefore it is important to make distinction between them and to describe preventive maintenance process. To have a better overview, the Figure 1 presents Service Support segment of ITIL process model with Incident and Problem Management processes in conjunction to other parts of Service Support set.

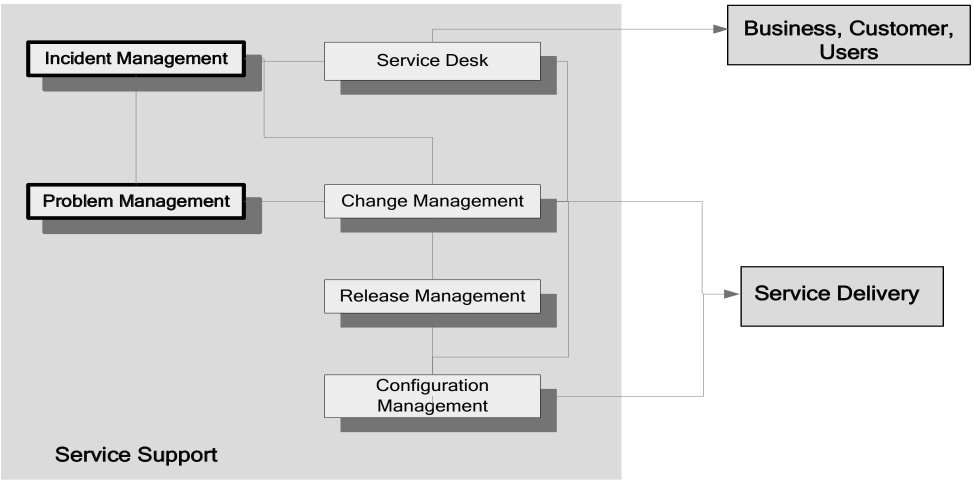

**Figure 1.** Service Support segment of ITIL process model with Incident and Problem Management processes and their conjunction

As Incident and Problem Management processes are described in detail in [21] the main difference can be seen in the approach to problem/incident resolution. Incident Management process is oriented to be effective in quick resolution of incident and its reduction of any adverse impact to the service. On the other hand, Problem Management process is primarily aimed at globally preventing and reducing amount of incidents by organizing its tasks toward identification of actual cause of a problem. As illustrated on Figure 1, Problem Management uses information provided by Incident Management and Change Management (that receives inputs from various sources).

Proactive approach is characterized with performing actions before a situation becomes a source of confrontation or crisis and enables applying preventive maintenance process to the system. It has been known that incidents are not easily predictable, making estimation efforts difficult and for the great part inaccurate. Compared to other types of maintenance all proactive activities can be planned and organized with greater precision. Reactive measures and technologies are better understood as they have been present longer and are widely deployed. The initial costs involved with a reactive approach are lower than those associated with creating a proactive system. Making the move to a proactive system requires a substantial investment, but will positive response as long run investment [12].

It is important that organization provides solutions for preventive maintenance tasks with great elasticity. Organization elasticity can be described as the ability of an enterprise to respond flexibly and gracefully to changing business and/or technological conditions without disrupting operations [2]. IT executives should therefore build elasticity-related initiatives upon specific business needs and benefits, to assure initial and long-term success and support across the enterprise. However, elasticity must be delivered in terms that both IT and non-IT personnel can understand and appreciate.

## 4. THE METAMODEL OF THE PROBLEM MANAGEMENT DOMAIN

Above in this paper we have briefly introduced the concepts of the problem management, particularly based on the ITIL framework. Today ITIL is a commonly accepted reference for different industrial implementations and applications. However, different implementations handle the ITIL's concepts differently and have their own conceptual world. Their specifications and models deal with different abstraction levels; in one case we have a textual description, in other a detailed design model or computer program accomplished with user's manual.

It is thus interesting to bring up a universal metamodel, adequate for better insights, comparison, interoperability, integration and further development.

Generally, a metamodel is the underlying model of all models and represents concepts, relations between concepts, frames, rules, constrains and theories, applicable and useful for the modelling in a predefined class of problems. While a model is an abstraction of phenomena in the real world, a metamodel is an abstraction of the model itself. A metamodel comprises an explicit description (formalized specification) of constructs, rules and notation for building domain-specific models.

Metamodeling addresses the problem of different abstraction mechanisms concerning information at different abstraction levels and transition from one abstraction level to another. The descriptions of concepts generate metadata. This metadata are considered as a classifier for a concept and its instances. A classifier can in turn be an instance of a higher-level classifier, which is a part of the higher-level meta-meta model.

Analogue to other domains, the role of metamodels of problem management is:

- Definition, representation, diagrammatical visualisation and gaining of understanding of problem management concepts, structure and behaviour,
- Comparison, evaluation and benchmarking of different project management applications and tools,
- Technology-independent platform for development of ITIL based models and applications
- High level integration model for integration of problem management and other ITSM sub systems,
- Integration platform for the exchange of problem management models that are specified in different languages and methods.

Although the concept and the theory of metamodels and metamodeling are widely discussed and applied in many scientific, business and real life domains, they do not exist in a strict, universal form. Metamodeling theories, methods, style and notation are growing in the frame of different domains and thus deviate. The difficulty of conceptualisation and building of metamodels lies in multiple aspects, first of all in different semantic framework (terminology, definitions, rules etc.) and notions and documentation of different systems. Therefore the methods of information abstraction and conceptualisation play the main role in the context of designing of metamodels.

As a part of our research we developed the metamodel of the Problem Management part of the Information Technology Infrastructure Library (ITIL). The metamodel is presented in an object-oriented fashion by using structure (class) diagrams conform to the OMG’s Unified Modelling Language (UML) notation [14]. Except of ITIL, we have also referenced research efforts in the domain of metamodeling in software development and IT related services. We took into consideration especially these which take parts of the ITIL framework in a relation to OMG’s MOF (Meta Object Facilities) [15], which is an abstract framework for defining and managing metamodels, neutral of any technology. We found some ideas in the management of the product engineering process, as treated in the OMG’s Product Data Management Enablers Specification [13].

According to different approaches, a metamodel may have different components: data and process; structure and behaviour; domain, requirements and transaction etc.

Figure 2 presents basic information (meta-data) structure of the metamodel concerning ITIL Problem Management domain, and related Incident and Change Management.

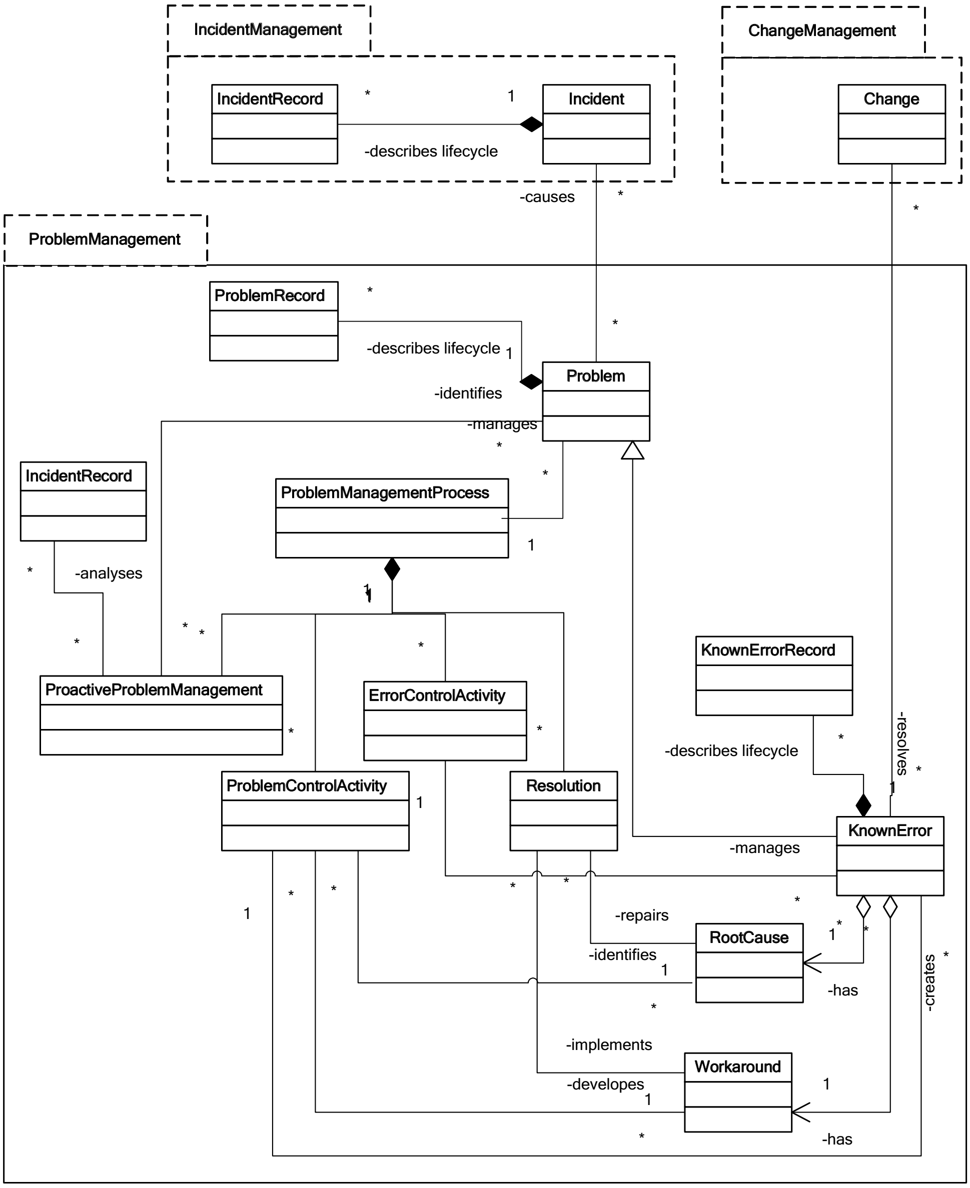

**Figure 2.** Basic metamodel of the ITIL based Problem Management domain, and related Incident and Change Management

Definitions of basic concepts presented on Figure 2 are as follows [16, 17]:

- *Change* - The addition, modification or removal of anything that could have an effect on *IT Services*. The *Scope* should include all *Configuration Items*, *Processes*, *Documentation* etc.
- *Error Control* - The Activity responsible for managing *Known Errors* until they are *Resolved* by the successful implementation of *Changes*.
- *Incident* - An unplanned interruption to an *IT Service* or reduction in the *Quality* of an *IT Service*. Any event which could affect an *IT Service* in the future is also an Incident. For example *Failure* of one disk from a mirror set.
- *Incident Record* - A *Record* containing the details of an *Incident*. Each *Incident* record documents the *Lifecycle* of a single *Incident*.
- *Known Error (KE)* - A *Problem* that has a documented *Root Cause* and a *Workaround*. Known Errors are created by *Problem Control* and are managed throughout their *Lifecycle* by *Error Control*. Known Errors may also be identified by *Development* or *Suppliers*.
- *Known Error Record* - A *Record* containing the details of a *Known Error*. Each *Known Error Record* documents the *Lifecycle* of a *Known Error*, including the *Status*, *Root Cause* and *Workaround*. In some implementations a *Known Error* is documented using additional fields in a *Problem Record*.
- *Proactive Problem Management* is the part of the *Problem Management Process*. The *Objective* of Proactive Problem Management is to identify *Problems* that might otherwise be missed. Proactive Problem Management analyses *Incident Records*, and uses data collected by other *IT Service Management Processes* to identify trends or significant problems.
- *Problem* - The root cause of one or more incidents.
- *Problem Control* - Part of the *Problem Management* Process. Problem Control is the *Activity* responsible for identifying the *Root Cause* and developing a *Workaround* or *Structural Solution* for a Problem.
- *Problem Management* - The *Process* responsible for managing the *Lifecycle* of all *Problems*. The primary objectives of Problem Management are to prevent *Incidents* from happening, and to minimise the *Impact* of *Incidents* that cannot be prevented. Problem Management includes *Problem Control, Error Control* and *Proactive Problem Management*.
- *Problem Record* - A *Record* containing the details of a *Problem*. Each Problem Record documents the *Lifecycle* of a single *Problem*.
- *Resolution* - Action taken to repair the *Root Cause* of an *Incident* or *Problem*, or to implement a *Workaround*.
- *Root Cause* - The underlying or original cause of an *Incident* or *Problem*.
- *Workaround* - Reducing or eliminating the *Impact* of an *Incident* or *Problem* for which a full *Resolution* is not yet available. For example, by restarting a failed *Configuration Item*. Workarounds for *Problems* are documented in Known Error

Records. Workarounds for *Incidents* that do not have associated Problem Records are documented in the *Incident Record*.

Definitions of some ITIL concepts are different as compared with other standards. For example, in ISO/IEC 20000 Resolution Processes is the Process group that includes Incident and Problem Management. So the metamodel can be used for comparison of different approaches and frameworks.

## 5. RECOGNITION OF CURRENT MAINTENANCE LEVEL

The successful implementation of best predictive and preventive network maintenance practices will generally undergo various stages, including the planning phase, compilation of best practices, documentation, and finally the dissemination and implementation phase. This whole process is both incremental and iterative and should be carefully monitored and controlled to ensure that best practices are both followed and implemented [7]. According to [2] most organizations are at one of three stages of maturity regarding their Incident and Problem Management. These stages of maturity can be described as:

- Reactive incident handling,
- Reactive problem resolution,
- Proactive problem management.

### *5.1. REACTIVE INCIDENT HANDLING*

Reactive incident handling is the first stage of maintenance maturity. Its goal is to create controlled, predictable incident resolution process. At the beginning it is required to create single point of contact (help desk, service support desk) that consolidates user requests from multiple sources and maintains communication about the status of each request throughout the incident life cycle. By using help desk tool, systematical record of incident and automatic generation of incident tickets can be established including relevant current and historical asset and user data. It is necessary to assess the impact of an incident on key business services and according to that to determine priority, classification and routing to appropriate support area based on available skill levels and areas of expertise. The above-mentioned efforts and the knowledge derived from them should be enough (or used as guidelines) to implement a consistent, automation-enabled Incident Management process driven by best practices and business requirements.

### *5.2. REACTIVE PROBLEM RESOLUTION*

The goal of this stage of maturity is to create stabilized, refined infrastructure for problem management. The first step toward the mentioned goal is to adopt automated tools to distinguish between single-occurrence incidents and deeper, long-term problems requiring in-depth root analyses. It is necessary to ensure that tools and processes gather and make readily available historical data about all incidents, including related asset, change, and/or configuration items and the results of any previously tried or used workarounds. Through the investigation and diagnosis process it is advisable to identify root causes and track the classification, urgency and status of both the problem and the underlying known error or errors with the goal to ensure timely and appropriate action. The previously mentioned efforts and knowledge gained from the above mentioned actions should be used to establish and implement Problem Management process driven by best practices and business requirements.

### *5.3. PROACTIVE INCIDENT AND PROBLEM RESOLUTION*

It is not easy to reach this stage of maintenance maturity because it requires a difficultly achievable goal of creating high-performance *proactive* problem resolution maintenance. The first thing that has to be done to get closer to the above mentioned goal is identification of lines of business (LOBs) and/or business processes that are affected by recurring incidents or failures and problems, including priority and status information. It is recommendable to determine if there are trends in asset-related issues, change requests and tasks, and/or specific incident and problem causes that warrant further investigation. Providing historical data on the underlying infrastructure, including the schedule of past planed and unplanned changes and the configuration items involved, can help in identification of root causes. Development of policies and tools that make all relevant information consistently, easily, and quickly accessible to personnel involved directly in Incident and Problem Management, as well as affected LOB decision-makers and senior executives within and beyond technological level (IT or else) can be done. Recommendable thing to do is integration of policies, procedures, processes, and solutions that enable mentioned steps with one another and with larger technological and business architectures.

Enterprise needs to evolve, grow and repeat the above steps/recommendations in order to develop and replicate proactive Incident and Problem Management process that reduce the overall number of reported incidents and problems and in order to help to raise and maintain service levels.

## 6. TOWARD HIGHER MAINTENANCE LEVEL

In this section we will describe the recommendation how to improve current maintenance and valorize it by reducing number of incidents and increasing system stability.

The difference between Incident Management and Problem Management has already been described in section 3. Incident Management process is oriented to be effective in quick resolution of incident and its reduction of any adverse impact to the service. On the other hand, Problem Management process is more oriented to globally prevent and reduce amount of incidents in the way to organize it tasks toward identification and of actual cause of problem. Problem Management focuses on minimizing the adverse impact of errors within the enterprise infrastructure through root cause analysis and on preventing recurring incidents related to these errors. Problem management relies upon historical data on changes, incidents, and users that may be related to the problem [2]. As mentioned in section 5, enterprise maintenance can fit in one of the stages of maturity or between. Most enterprises, which have ambition to exist on the modern market, have already developed reactive incident resolution by using single point of contact, tools and analytical methods for incident classification and monitoring. Nevertheless, they do not have adequate elasticity that can bring greater business benefit and develop maintenance performance to fit actual maintenance challenges.

Evolution to higher maintenance level requires adequate investments and plans with achievable business goals and feasible time frame. At this point it is important to develop incident root cause analysis approach that can summarize and evaluate incidents. This would be the first step in reaching reactive problem resolution level. Currently many organizations offer their solutions how to monitor and analyze incidents, or patented algorithms for trend analysis [1, 4, 21, 22], yet it is important to distinguish incidents that have single occurrence from those that have deeper and long-term consequences on business benefit. Such software solutions can be useful, nevertheless it would be wise to precisely support organization needs and, if necessary, even develop own solutions to adequately fit business needs.

As the next step how an organization can approach proactive incident and problem resolution level, we would like to emphasize the possibility of upgrading maintenance performance by applying solutions or, where possible, tools that are able to speed up root cause analysis. In some of the already mentioned software solutions there are ideas how it is possible to do so or, if it is not possible to automate such process, the recommendation is to perform that job "manually". Organizations can assemble a team of highly specialized and experienced personnel with the task to analyze, evaluate, classify, diagnose and change incidents and imperfections in system with the ultimate goal to increase system stability and reduce overall number of incidents. According to Figure 1, that personnel should be part of Problem Management process and it should work tightly with the personnel that is part of Incident Management and Change Management process. In some networks that job can be done by AI agents [7, 8] nevertheless in networks that require higher level of intelligent solutions human work force cannot be avoided (Figure 3).

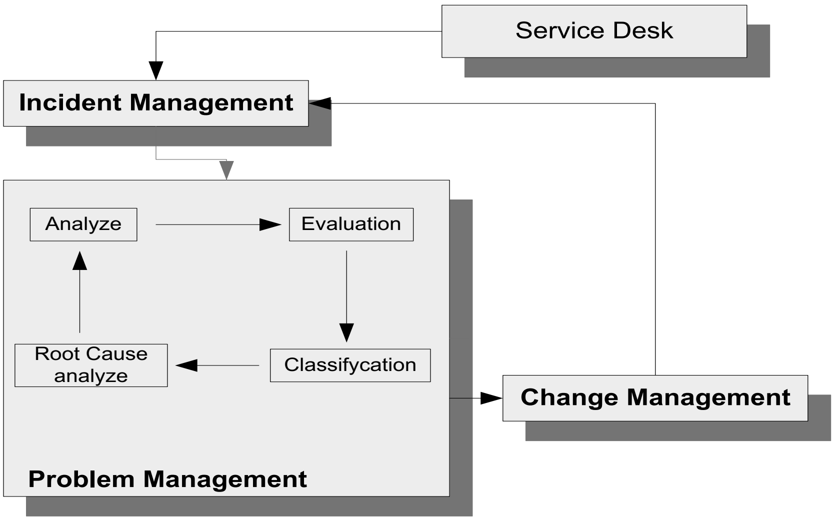

**Figure 3.** Activities in Problem Management process for proactive approach to incident and problem resolution

The Figure 3 describes our suggestion regarding proactive activities imbedded in Problem Management process with the goal to reduce overall number of incident through incident and problem resolution process, root cause analysis and Change Management process activities. Incidents information is collected and sorted by tools that are used in Service Desk and Incident Management process. After that, historical data of incidents are analyzed by group of specialists with single or multiple occurrence determination. Before classification, when priority and solution significance is determined, it is necessary to evaluate business impact of incidents that are analyzed. Root cause analysis is the main point where proactive solutions are determined and provided. After the root cause analysis, the proposal for proactive activities is communicated with Change Management process that determines changes necessity and evaluates proactive activities for impact on the other parts of services. After the evaluation, proactive change resolutions are imbedded into system by Incident Management. In that way, we can increase organizations' flexibility and speed up resolution and incident implementation time, especially in large enterprises without enough flexibility in process of change implementation.

## 7. PERFORMANCE MEASURING AND MANAGEMENT

Moving from reactive to proactive maintenance management requires time, money, human resources, as well as initial and continued support from management. Before improving a process, it is necessary to define the improvement. That definition will lead to the identification of a measurement, or metric. Instead of intuitive expectations of benefits, tangible and objective performance facts are needed. Therefore, the selection of appropriate metrics is an essential starting point for process improvement.

Metrics are a system of parameters or ways of quantitative assessment of a process that is to be measured, along with the processes to carry out such measurement. Metrics define what is to be measured. Metrics are usually specialized by the subject area, in which case they are valid only within certain domain and cannot be directly benchmarked or interpreted outside it. Although attractive, implementation of metrics can be a two-egged sword because questionable and inaccurate indicators can cause bad management decisions. Depending on the type of data that are collected, a given process may be measurable in many different ways.

Based on current research, we organized metrics into some distinct and recognizable operational and financial categories. For these we developed Key Performance Indicators (KPIs), significant factors that directly and indirectly influence the effectiveness of a product or process. They are used on its own, or in combination with other key performance indicators, to monitor how well a business is achieving its quantifiable objectives. The basic idea of KPIs is to provide some mechanism for quantification of the maintenance process. As targets, KPIs must be widely understandable and accepted concepts, appropriate to be set within an SLA.

Listed are some recommended KPIs grouped by areas of management:

*1. Availability* is a measure of time that a service unit or facility is capable of providing service, whether or not it is actually in service. Typically this measure is expressed as a percent available for the period under consideration. An *Uptime* is calculated as total time minus all known losses due to equipment failures measured in time. Extended losses could include also losses due to process set-up, start-ups, adjustments - breaks, lunch, weekends etc.

- Availability = Uptime / Total time
- Number of hours (minutes) off – Total hours (or minutes) when some equipment or system was unable to perform its normal functionality
- Lost hours rate - Number of hours (minutes) off / Number of hours operating
- Number of log incidents - Any incident requiring some delivery of maintenance services
- Incident rate = Number of log incidents / Number of hours operating

*2. Reliability* is the probability of performing a specified function without failure under given conditions for a specified period of time.

- *MTBF (mean time between failures)* is the average time a system will operate without a failure. The MTBF is a commonly-quoted reliability statistic, and is usually expressed in hours (even intervals on the order of years are instead typically expressed in terms of thousands of hours [22],

- *MTTR (mean time to repair)* is the average amount of time required to resolve most hardware or software problems with a given device or system and indicates its maintainability,
- *MTBR (mean time between repairs)* = MTBF – MTTR,
- *OEE (overall equipment effectiveness)* is a combined formula that shows the overall performance of a single piece of equipment, or even an entire system, by multiplying Availability x Performance x Quality. OEE has been initially developed for production and not for services. For that reason we have redefined availability as percent of scheduled service time available), performance rate as percent of outputs (service units) delivered compared to standard and quality as percent of outputs delivered compared to outputs started.

*3. Productivity* is used to measure the efficiency of delivery of services, and is most often expressed as a ratio of outputs (delivered services) over time and other resource inputs used in accomplishing the assigned task. It is often considered as output per person-hour. Outputs generally include all labour (hours worked, including overtime) or Equivalent service units (ESUs) delivered. ESUs are standardized standard service contents used to aggregate delivered work when there is a service mix with different labour content.

- *Labor Productivity* = Outputs (service units) delivered / Labor Hours,
- *Crew efficiency* = Actual labor hours on scheduled work / Estimated labor hours,
- *Value added cycle time* – a portion of the total cycle time where value is actually added to the product or service,
- *Maintenance Process Efficiency = Maintenance* costs / Total revenue

  or Maintenance costs per delivered service unit.

*4. Planning and Management Quality* – the basic idea is to predict and plan as much as possible so that it expresses the proportion of total maintenance time vs. corrective or unplanned actions.

- *Involvement of the preventive & predictive maintenance (PPM)* = PPM labor hours or work orders / Emergency labor hours or work orders,
- *Work order discipline* = Labor hours accounted on work orders / Total labor hours,
- Planned labour hours / Scheduled labor hours,
- Unplanned labour hours / Total labor hours.

*5. Management Performance*

- Delivery on-time % - percent of service deliveries made on or before the due date,
- Number of complaints - total number of warranty claims or "Things Gone Wrong" (TGW's) reported in some period, may be divided by the total number of work orders or service hours,

- Customer satisfaction - may be measured directly by survey and expressed as a percentage, such as Percent of satisfied customers.

Based on actual empirical research, the proposed metric gives promising results.

## 8. CONCLUSION

In this paper we have covered recent trends in proactive approach in communication network maintenance, guidelines and recommendations for maintenance level recognition and improvements, metrics that influence product or process effectiveness – all that with the goal to set up maintenance to a higher level. Instituting a genuine and effective preventive network maintenance program is a key step toward achieving world-class maintenance status. The transition toward preventive network maintenance requires careful planning, considerable effort and most importantly, a strong commitment from top management and other levels of the organization. Benefits of proactive approach in maintenance can be found in continuous and more stabile services with less incidents and problems, increased productivity of support specialists, error prevention and better control of services through improved management information and systematic approach.

We have briefly introduced the concept of the problem management based on the ITIL framework, which is today a commonly accepted reference but different industrial implementations and applications. The approach we proposed and elaborated in this paper is the construction of a metamodel of the problem management of information technology, particularly the proactive problem management. The metamodel is derived from the original ITIL specification and presented in an object-oriented fashion by using structure (class) diagrams conform to UML notation. The metamodel can be used for better insights, comparison, interoperability, integration and further development.

Individual businesses areas and specific needs of the company may inspire managers to choose the best course of action via proactive or reactive approach. In the end, an effective maintenance management asks for a comprehensive management approach that applies both proactive and reactive components.

Based on current research, appropriate metrics based on the concept of Key Performance Indicators is suggested.

As maintenance is an important topic in network management we hope that this paper will motivate new research and case studies related to maintenance proactive approach. From our point of interest, current research is in the field of develop integrated metamodels of ITIL structure and behaviour.

## REFERENCES

[1] BEZ Systems, Inc. Proactively Managing Data Service Delivery to the Business, White paper, www.bez.com

[2] Dortch, M.: The Elastic Enterprise in Action: IT-Empowered Incident and Problem Management. Custom Research Note, Robert Frances Group, 2005

[3] Hanemann, A., Sailer, M., Schmitz, D.: Assured Service Quality by Improved Fault Management. Leibniz Supercomputer Center and University of Munich, 2004

[4] Identify, How to Accelerate Your Application Problem Resolution Process, White paper www.identify.com

[5] Ishikawa, H.; Nakajima, T.; Oikawa, S.; Hirotsu, T.: Proactive Operating System Recovery. Proceedings of the twentieth ACM symposium on Operating systems principles, Brighton, UK, 2005

[6] IT Infrastructure Library, Office of Government Commerce and IT Service Management Forum http://www.itil.co.uk.

[7] Kamoun F.: Toward Best Maintenance Practices in Communication Network Management, International Journal of Network Management, 2005

[8] Leckie, C.: Experience and trends in AI for network monitoring and diagnosis, In Proceedings of the IJCAI95 workshop on AI in Distributed Information Networks, Montreal, Canada, 1995

[9] Maintenance Philosophy for Telecommunication Networks, ITU/CCITT Recommendation M.20, 1992.

[10] Maintenance: International Telephone circuits: Maintenance Methods, ITU/CCITT Recommendation M.733, 1993.

[11] Misra, K.., Arun, Bhatt, P., Shroff, G.: Dynamics of Software Maintenance. National Institute of Technology, Allahabad, India

[12] nCircle Network Security: Proactive Network Security: Making your Network Unassailable, http://www.ncircle.com

[13] Object Management Group (OMG): Product Data Management Enablers Specification. Version 1.3, http://www.omg.org/technology/documents/, November 2000

[14] Object Management Group (OMG): Unified Modeling Language (UML): Superstructure, version 2.0, http://www.omg.org, August, 2005

[15] Object Management Group (OMG): Meta Object Facility (MOF) Core Specification. v2.0, January 2006

[16] Office of Government Commerce (OGC): ITIL Service Delivery. The Stationery Office Books ISBN 0113300174, 2002

[17] Office of Government Commerce (OGC): ITIL Service Support. The Stationery Office Books ISBN 0113300158, 2002

[18] Qin, L., Kunz, T.: Pro-active Route Maintenance in DSR. Department of Systems and Computer Engineering, ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 6/3, 2002

[19] Strahonja, V., Saletović, K..: Improving Maintenance Performance With Incident and Problem Tracking Models, Journal of Information and Organizational Sciences, 2005

[20] Vaidyanathan, K., Harper, R.E., Hunter, S., Trivedi, K.S.: Analysis and Implementation of Software Rejuvenation in Cluster Systems, Proceedings of the 2001 ACM SIGMETRICS international conference on Measurement and modeling of computer systems, 2001

[21] Warren, G. et al.: Network simulation enhancing network management in real-time. ACM Transactions on Modeling and Computer Simulation, 14(2): 196–203, 2004

[22] www.moresteam.com/metrics.cfm (Lean Six Sigma Metrics Definitions)

**Received:** 14 March 2007

**Accepted:** 29 November 2007