ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 3 (2013) No. 04, pp. xxx-xxx

Analysis and Optimization of Alarms

Thirumalainambi Murugesh [1] and Chandrasekara A.S. Aiyer [2+]

[1] Integration Architect, IBM Australia, 601 Pacific Highway, St. Leonards, NSW 2065, Australia
[2] Architecture Group Manager, IBM Australia, 601 Pacific Highway, St. Leonards, NSW 2065, Australia

(*Received 20 June 2013, accepted 03 October 2013*)

Abstract. Modern state-of-art management software can manage thousands of multi-vendor devices through a single centralized remote console proactively and alert operators when there is an incident or even in advance with known symptoms that there is an incident going to happen. Even with the modern software, currently huge Telecom and service providers are facing a huge number of alarm floods to process every day. This paper examines the need for alarm management, business benefits of alarm management, different kinds of alarms, state-of-art management software features, assessment of currently deployed alarm management system and a description of a proven approach in terms of people, processes and technology that can be adopted to cut down the quantity of alarms and enhance the quality of alarms which will eventually lead up to increase in revenue and network availability time.

Keywords: Alarm management, Alarm assessment, Alarm management approach, Business benefits of alarm management.

1. Introduction

Network elements and communication systems are business critical components that need to be working 7x24 and fully available at all the time. The cost in terms of lost business or the effect on company image and customer satisfaction will be huge even if the network elements and systems stopped working even for a very short while. This can be avoided and easy to protect the revenue generating network reliability and uptime by proactively monitoring the health of network elements, servers and communication systems day and night and all year around. Modern state of art management software [1] can manage thousands of multi-vendor devices through a single centralized remote console proactively and alert operators when there is an incident or even in advance with known symptoms that there is an incident going to happen. In [2] Bob Berry had stated that many telecoms and enterprise service providers are not investing in network monitoring equipment. But they're the ones with failing service levels, fleeing customers and declining profits.

In the following figure logical representation of a network management model [3] is shown with three layers model of Element management layer, Network management layer and service management layer with manager of managers (MOM) at the top for receiving alarms from underlying components, enrich the events by correlating them and present to the Network Operations Centre (NOC) operators business impacting service views rather than showing discrete alarms coming from every element managers in the element manager layer.

[+] Corresponding authors. Tel.: +61 402 268 648, +61 414 886 251.
E-mail address: thirumalainambi.murugesh@au1.ibm.com, aiyerch@au1.ibm.com.

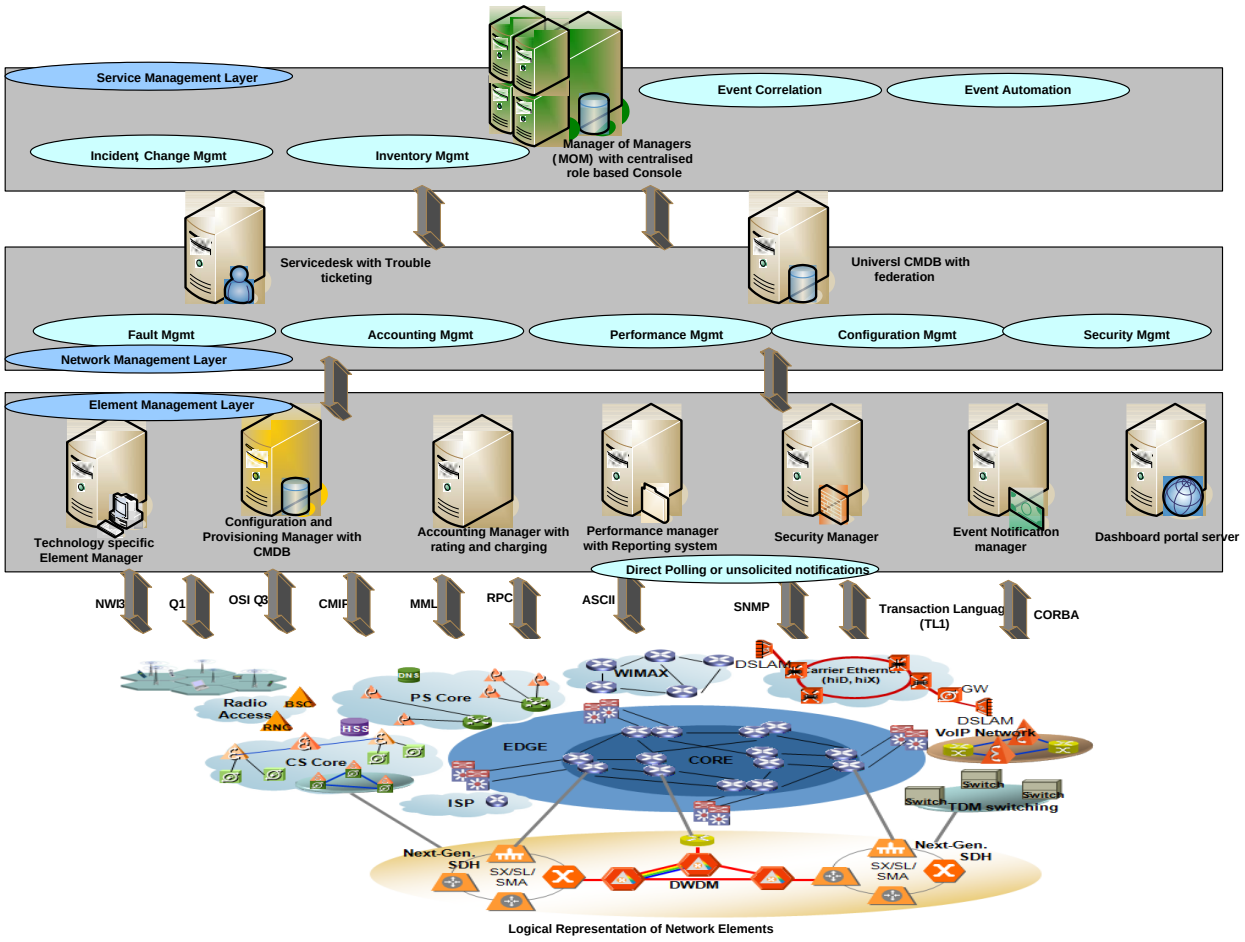


Fig. 1: Logical representation of integrated network management systems architecture.

In the recent years a strong growth of the communication networks [9] has taken place, with significant increments in the number of users, vendors, offered services [4], available technologies and quality demands (99.999% uptime) has increased the communication networks complexity very strongly. Today's network architectures complexity forces the alarm management to be aided by the state-of-the-art software. This paper presents the

- need for alarm management;
- business benefits of alarm management;
- different kinds of alarms;
- state-of-the-art management software features;
- assessment of currently deployed alarm management system and
- case study on alarm analysis and optimization for alarm environment that handled IP, Transmission and Mobile infrastructure and application alarms for Telecommunications Service Provider in Australia.

Alarm analysis and optimization approach is explained in terms of people, processes and technology to cut down the quantity of alarms and enhance the quality of alarms which eventually led up to increase in revenue and network availability time.

2. Why We Need An Effective Alarm Management?

With modern technologies and software integration, most of the vendors are able to add their own set of alarms for different state conditions of their products. As the addition of alarms doesn't cost much to the vendors and alarm implementers and alarm systems integrators rigorous analysis was not always applied in configuring the additional alarms, result in operators getting flood of uncorrelated alarms for a single incident.

Understanding the meaning of an alarm and the consequence of not responding to it, is crucial to an operator effectiveness. As an example when the primary fast link has failed with fall back to slow ISDN link for a customer site, whether the operator knows the impact of the alarm even though the network service was not down for the end customer.

Alarm management addresses the above issues by

- Developing a Master Alarm Plan (MAP);
- Reducing the noise and derived alarms with smart event correlation logics and help the operators to identify the root cause of the problem immediately;
- Enhancing the quality of the alarm by improving the alarm with additional meaningful message text in plain English and
- Helping the operators to start troubleshooting the incidents with instructions to launch diagnostic tools and suggestions to address the potential issues

In [5] Rick Dodd had mentioned monitoring revenue-generating equipment with simple summary alarms will give only node up/down status only but to get a complete picture, monitoring has to be done comprehensively from card level to site level including environmental alarms.

3. Business Benefits Of Effective Alarm Management

- NOC operators will be able to manage multi vendor devices and services provided on top of them through a single manager of managers (MOM) console, hence training and maintaining multiple vendor element managers' console is not necessary saving a huge operational expenses.
- NOC operators will be able to proactively monitor the network and promptly identify network majors as a result of improved correlation and root cause analysis.

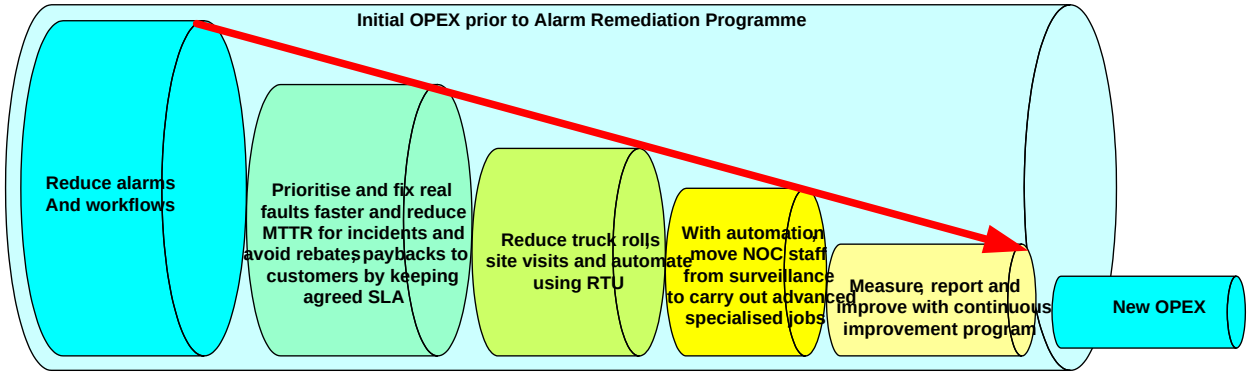


Fig. 2: Reduction of OPEX with alarm remediation programme.

- Factors impacting the reliability of Network elements will be picked up in advance with performance and threshold violations alarms and hence able to provide 99.999% reliable network uptime.
- Effective alarm management helps Business to develop trending patterns and analysis for capacity planning and forecasting.

- Development of intelligent filters, counters or qualifiers to filter nuisance alarms which will cut down the numbing barrage of meaningless alarms that distract NOC operators attention from critical Alarms which will lead them in missing business critical alarms.
- Enhancing the ability to perform, more automated root cause analysis which is essential to enable faster service restoration times which will help Business to minimize SLA penalties, and reduce downtime costs from service outages.
- Number of staff involved in managing alarms can be optimized and their knowledge and skills will be used in automation freeing them to do more specialized jobs.
- Able to keep uptime of the managed network elements at five 9 levels (99.999).
- Able to reduce the customer churn rate and increase customer base from industries competitors by improving network reliability and customer service through positive customer experience.
- Effective alarm management through implementation of Master Alarm Plan (MAP) will ensure the alarms are correctly configured with right severity, clear message text, and additional useful instructions for troubleshooting to enhance the operator effectiveness and control the process of adding new alarms with the introduction of new technology.
- Alarm systems will be able to handle the load easily without queuing up the incoming alarms and introducing a delay and able to handle additional customers growth without a need for additional infrastructure change.

4. Alarm and its types

Alarm messages are notifications either created by the element managers through its proactive polling for certain parameters on the managed object or notifications sent by the managed object through its agent (traps) by its watch dog daemon when performance and capacity threshold breaches occurred. These alarms are presented to the alarm management platform in one of the following sub categories

Status alarms:

- Service Affecting alarm events: These are messages that are presented to the platform that are affecting service.
- Non Service Affecting alarm events: These are messages that are presented to the platform, require action but are not service affecting (e.g.) Loss of IOF redundancy, IOF path switchover.

Threshold alarms:

Messages that do not produce an alarm event until a threshold has been crossed. These can be service or non-service affecting. Performance messages are defined as messages that report on the performance of the network element or platform. These messages should be mutually exclusive to alarm events. Performance threshold crossing alarms should be sent to the alarm platform so that Operators are made aware of poor performance issues.

Informational alarms:

These are defined as messages that may not be service affecting however they are required for future reporting, trending or post event fault analysis, isolation and rectification.

Environmental alarms:

These are defined messages that report on building and site alarms including commercial power availability, UPS battery level, rectifier, generators fuel level, site intrusion, open doors, fire alarms, heating, ventilation, air conditioning, temperature and humidity.

Noise alarms:

Alarms produced by network elements that are not useable in real-time surveillance or for trending analysis. These alarm messages should be blocked at the network element layer and not sent to the

centralized MOM alarm platform.

Derived alarms:

Alarms generated by the element manager system with user defined filters to create additional alarms upon seeing certain alarms in sequence in set time interval. As an example when the element manager receives alarms for low battery and low generator fuel, they will be assigned with warning severity but when they come in sequence within few minutes, the system will generate a critical alarm considering the situation.

Consequential alarms:

In a network management scenario, a fault usually leads to several consequential faults. This means that a single fault can create a large number of alarms, a so-called alarm flood.

5. State-of-the-art Alarm Management Software Features

It is not uncommon to see huge Telco and enterprise service providers are facing the challenge of processing over millions of alarms a day. Most of the modern state-of-the art management software provides the following features

- Role based client access [native java based client and web based client] is essential for managing the network environment in terms of configuration, maintenance, administration and support.
- Ensures all alarm life cycles are stored in the database for reporting and auditing purposes.
- Able to manage the alarms based on competency centre concept, follow the sun path or their combination to have distributed NOC centers
- Able to escalate the alarms to next level when the alarms stayed in active alarm browser for certain amount of time and not acknowledged by assigned operators group
- Able to create an incident by right click of the alarm manually in operator assisted fashion or create an incident automatically in the trouble ticketing system and exchange updates bi-directionally.
- Comes with out-of-box correlation circuits with filter rules which can be customized or added additional rules to filter out nuisance, consequential and derived alarms with an ease-of-use GUI.
- Users client GUI with the flexibility of creating different views to suit their filter requirements and ability to launch alarm object sensitive tools and smart actions
- Users client GUI with the flexibility to sort and search alarms with different parameters including severity, managed object, customer, date range etc.
- Alarm view showing list of outstanding active alarms with a green/red traffic light indicator view. With this even if the operator acknowledges the alarm, the object will show still red until comes back to normal.
- Heart-beat or watch dog monitoring on the alarm management system and its components to make sure the alarm system is functioning as expected.
- Manager of Managers [MOM] is able to receive alarms from any underlying element managers which operate with different kinds of protocols through smooth and easy integration.
- Able to integrate with email, SMS gateways to send automated email and SMS notifications.
- Able to implement Master Alarm Plan covering configuration, administration and support of event specific parameters such as mapping of fields (severity, additional useful text, probable cause etc).
- Alarm systems are scalable, reliable, redundant and the components are modular to support future growth and additional load without re-doing the whole implementation and integration.

- Alarm systems are secure with strong authentication and access control, customer segregation policies in place to prevent un-authorized users accessing the Business critical or competitive information.

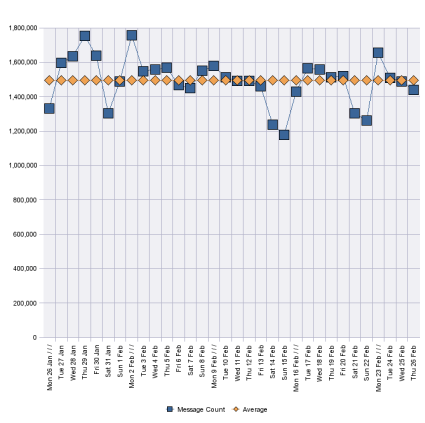
6. Case Study on Alarm Analysis and Optimisation

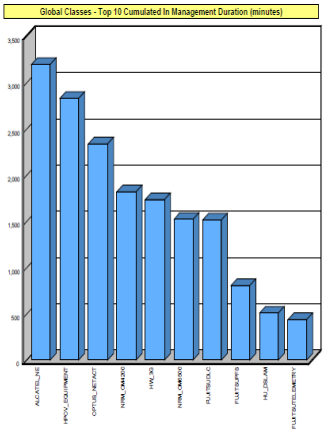
Ideally every Business like to have one genuine root cause alarm per incident and it may not be the case due to the network complexity and multi vendor products and element managers integration. The quality of alarms is bad if the nuisance and consequence alarms are not filtered at element managers, the quantity of alarms coming from every layer of the network management architecture model will add up to a flood of alarms for an incident. In this section we present the results of analysis and optimization of alarms we had conducted recently for a major Australian Telecommunications service provider.

6.1. Analysis Of Alarms

There are many out-of-box reporting solutions on the market that gives the flexibility to build Business Object Universes for the alarms data warehouse and allow end users to pass different parameters in the selection window to produce required reports. Most common reports that will help to identify the current state of alarms are the following which can be scheduled to run on daily basis with a time period of last one day, last one week, and last one month. These reports give a clear indication of pain points that need immediate attention.

- Top 100 managed objects causing most number of alarms
- Top 20 noise alarms
- Top twenty probable causes that generated the number of alarms
- Alarms by severity distribution against date and time
- Alarms load handled by NOC operators
- Alarms by top 15 services
- Alarms resolution time by severity
- Alarms resolution time by operators
- Alarm resolution time trend
- Alarms by customers
- Alarms trend by severity
- Alarms resolution against Customer SLA time
- Alarm queue trend
- Alarm systems performance in terms of CPU, memory, disk capacity and network
- Alarm trend showing average and peaks





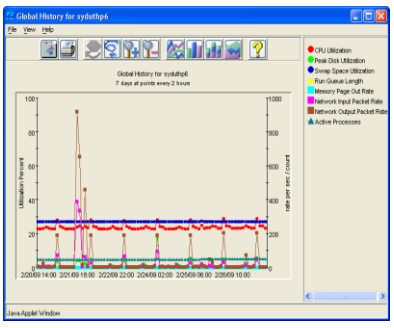


Fig. 3: Graphs showing daily message arrival with average Top ten reports and alarm system performance.

If there is no reporting package solution already deployed in the environment, it is easy to develop custom SQL scripts by looking at the alarm database schema as shown below.

```
select OPC_OP.OPC_NODE_NAMES.NODE_NAME,
         count(*) "No of alarms per node"
  from OPC_OP.OPC_NODE_NAMES,OPC_OP.OPC_HIST_MESSAGES
where OPC_OP.OPC_NODE_NAMES.NODE_ID=OPC_OP.OPC_HIST_MESSAGES.NODE_ID
   and OPC_HIST_MESSAGES.LOCAL_RECEIVING_TIME BETWEEN
       trunc(sysdate-1) and trunc(sysdate)
group by OPC_OP.OPC_NODE_NAMES.NODE_NAME
order by count(*) DESC;
```

NODE_GROUP_NAME	QTY
Infrastructure	386
OPI Plus	280
eFinity	230
Backup Network	197
Management Servers	196
St Georege Bank (stg)	148
o22rrnms06	142
o22rrnms06 dsl	139
Mascot Servers	137
VPN_MRS_DSL	120
IP Centrex	106
Wesley Central (wes)	68
Network Com (ntk)	66
Supre(sr9)	62
Tandem VCCS	54
o22rrovomscl	49

MSG_SOURCE_NAME	DESCRIPTION	COUNT(*)
snmp	OV_Node_Down	62
UNIX_SNMP_Collection_threshold	L2TP_Tunnel_Down_Partial	55
UNIX_SNMP_Collection_threshold	L2TP_Tunnel_Up_All	41
snmp	OV_dataWarehouseMaintError	11
OPIPlus_TNT_ModemBank	TNT_Faulty_Modem_Polling	9
OPI_Radius_DR	altSwSlbRealServerServiceUp	6
snmp	OV_IF_Intermittent	4
snmp	OV_Node_Up	4
snmp	OV_ResumeSuccess	4
NNM	OV_IF_Flags_Chg	3
OPI_Radius_DR	altSwSlbRealServerService_down	3
UNIX_SNMP_Collection_threshold	SmartPayFw_Load15mins_High	2
snmp	OV_DaemonTerminated	2
snmp	frDLCIStatusChange_inactiveandInvalid	2
Compaq	cpqHo2AppErrorTrap	1
Juniper_JnxVPN	jnxVpnIfDown_pe	1

With the above reports we are able to establish a baseline on the current state of alarms. As shown below from the report for 11 days NOC operators received over a million alarms which gives an alarm frequency of roughly 70 alarms per minute.

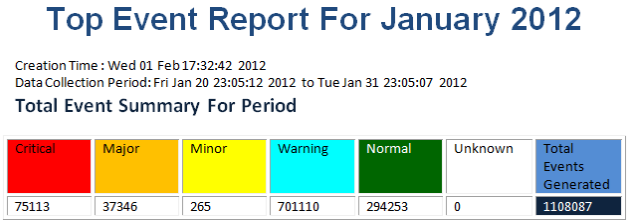


Fig. 4: BOE Report showing Alarm Summary report.

This was unmanageable by the operators and they were missing genuine critical alarms and the alarm system was struggling to cope up with the amount of alarms coming for processing with various defined filters and correlation logics which led to messages end up in queue before showing up in the alarm screen for operators.

We analyzed the alarms in terms of People, Processes and Technology. They are covered in terms of Alarm flow management, Alarm handling process, Data aggregation and correlation, Fault Escalation, Fault Resolution, Fault metrics, FM organization and site visit reduction. Their definition are given in the following table.

Category	Description

Alarm Flow Management	Are there procedures and practices in place to manage the alarm flow to users in the front office and back office functions so that load on users is as required and not just all?. Is there sufficient review and assigned roles to enforce improvement?.
Alarm handling Process	Is the alarm handling (NOC) efficient to detect, diagnose and resolve or escalate faults derived from alarm indication?. Are practices clear and reviewed for improvement?
Data Aggregation and Correlation	Are there practices that review the NW alarm data as well as other sources to help detect quiet, transient or persistent faults in both reactive and proactive roles?. Are there assigned roles to review root cause rules to minimize noise and strong linkage between front desk users and the root cause roles?.
Fault Escalation	Is there clear and efficient escalation practices and organization to allow faults to be resolved efficiently and with the minimal steps?. Is the escalation steps minimized, containing required information and reviewed to improve?.
Fault Resolution	Are there sufficient tools and practices in place to maximize resolution capabilities and tracking to keep downtime and case lifetimes to a minimum?
Fault Metrics	Is the client actively reviewing all steps in the Fault management process to check for efficiency issues so that better procedures and practices can be advised?
FM Organization	is the FM organization clear to all and in a framework that best suits the business model and client demographics?
Site Visit Reduction	Are there procedures and activities in place to reduce and minimize the need for physical site attendance to for reaction fault resolution. Are non-productive resolutions at site (no fault found, self clear, reset etc) analyzed and reduced?.

Table. 1: Alarm Analysis Radar Chart Categories Definition.

By interviewing various people from the organization involved in the alarm and fault management, assessing processes in place and alarm systems design, implementation and operations model, health score can be collected and plotted through the radar chart against the following field values Competence, Processes, Reducing errors and re-work, Resources, Roadmap and Tools. Their definition are given below in the following table.

Field	Description
Competence	Is there sufficient competence in the field to yield benefit?
Processes	Are there processes to enforce and harness the benefits in the field?
Reducing errors and re-work	Is there sufficient focus on reducing errors and re-work through proactive and reactive processes?
Resources	Is there sufficient resource in the field to yield benefit?
Roadmap	Is there a vision to further improve this field in operations?.
Tools	Are there sufficient tools available to deliver the required tasks and are these centralized or easily accessed?.

Table. 2: Alarm Analysis Radar Chart Fields Definition.

From the results, score was plotted in Radar Chart for each category against the field values.

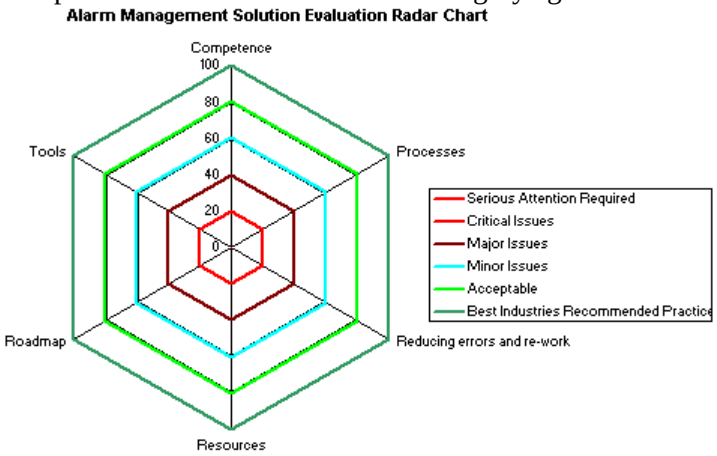


Fig. 5: Alarm Analysis Radar Chart Template.

The following section describes the assessment procedure to get the score. The score will be used in radar charts to assess each category mentioned in the table-1 against the fields mentioned in table-2.

6.2. Alarm Management System Assessment – People

To analyze whether the alarm solution in place is adequate enough in terms of People aspect, following questions were asked to the Business to evaluate the score for radar charts.

- Is the accountability in terms of ownership to develop, test and put into production for alarm plan is very clear?
- Are the NOC operators aware of all the features of alarm system presents to them to make their job easier?
- Are the NOC operators certified against vendor certification?
- Are the NOC operators aware of the team and escalation structure?
- Are the NOC operators able to identify the troubleshooting diagnostics tools and execute them remotely from the management system?
- Is there a dedicated person or a team of people to analyze the daily and weekly alarm trend and reports?
- Are the alarm plans available at a central location which can be accesses by the operators with relevant authentication from the alarm?
- Are the NMC and technical specialists receiving regular daily and weekly scheduled alarm reports covering top twenty probable causes, specific problem codes and managed objects?
- Is it possible to provide feedback on the alarm patterns and trends for certain incidents to Technology Specialists by NOC operators?
- Are the NOC operators managing the alarms with their own way of intelligence gained through experience than system level filters applied at the alarm systems?
- Are the NOC operators able to understand the criticality and business impact of the alarm?
- Are the NOC operators able to launch alarm sensitive and managed object context tools and applications from the console for troubleshooting and diagnosing the incident?
- Are the NOC operators able to add incident specific details in the operator notes of the alarm to pass the knowledge to others?

- Are NOC operators getting genuine one alarm per incident or flood of un-correlated alarms for all devices on its path?
- Are NOC operators getting alarm within 1 minute of incident occurrence time?

6.3. Alarm Management System Assessment - Processes

Following set of key questions were used to evaluate the current alarm management processes and charted using radar chart which gives a clear indication of current process health.

- Are there procedures and practices in place to manage the alarm flow to users in the NOC from Tech Specialists, Engineering Team and Vendors so that load on users is as required and not just all?. Is there sufficient review and assigned roles to enforce improvement?
- Is the alarm handling (NOC) efficient to detect, diagnose and resolve or escalate faults derived from alarm indication? Are practices clear and reviewed for improvement?
- Are there practices that review the Network alarm data as well as other sources to help detect alarm faults in both reactive and proactive roles? Are there assigned roles to review root causes to minimize noise alarms.
- Is there clear and efficient escalation practices and organization to allow faults to be resolved efficiently and with the minimal steps? Is the escalation steps minimized, containing required information and reviewed to improve?
- Are there sufficient tools and procedures in place to maximize resolution capabilities and tracking to keep downtime and case lifetimes to a minimum?
- Is the alarm management team actively reviewing all steps in the Fault Management (FM) process to check for efficiency issues so that better procedures and practices can be advised?
- Is the FM organization clear to all and in a framework that best suits the business model and Business demographics?
- Are there procedures and activities in place to reduce and minimize the need for physical site attendance to for reaction fault resolution? Are non-productive resolutions at site (no fault found, self clear, reset etc) analyzed and reduced?
- Is Master Alarm Plan covering the alarms, their severity, and message text to display to analysts and correlations used, value added information in each message to enhance NOC operators in troubleshooting present?
- Whether NOC operators are able to insert an incident into ticketing systems, send email and SMS notifications to relevant internal Specialists and impacted customers from the alarm screen?
- Whether the managed objects are not up to date in terms of decommissioned nodes are removed and to be managed nodes are rightly provisioned in element manager systems?

6.4. Alarm Management System Assessment – Technology

To analyze whether the alarm solution in place is adequate, following questions were asked to get the score to plot in radar chart.

- Is the managed objects in the alarm solution is accurate against inventory database?
- Is the trend of alarm is predictable that at certain date and time or during specific events the whole surveillance screen will be filled with thousands of alarms and operators clear them without going through but selecting all and acknowledging them?
- Are the top twenty alarms generating nodes on a daily basis and top twenty probable causes for generating those alarms are known?
- Are the provisioning alarms and scheduled maintenance alarms are not differentiated from service failure alarms and presented to NOC operators?

- Are the operators using multiple element managers' management console to view the alarms than a role based centralized single alarm console?
- Is the automatic incident creation and notification from the alarm system is not integrated or not working?
- Is the incident created in servicedesk is not getting update from the operator and closing upon acknowledging the alarm?
- Are the operators managing the network using their own experience to avoid missing SLAs?
- Is the total number of incidents created in servicedesk is not equal to the total number of alarms received?
- Is there a master alarm plan (MAP) covering alarm requirements, list of implemented alarms with set threshold limits and time, alarm management process etc available in a central repository accessible by operator upon authentication?
- Is there a web based document repository that contains vendor manuals, solution design guides, Operational guides, troubleshooting guides with role based access available?
- Is the Alarm server facing performance bottleneck issues in handling the load in terms of number of incoming alarms, processing them in terms of filtering, correlating them and reporting them to operators' consoles?
- Is the alarm server architecture able to handle growth due to its design limitations? (modular, scalable, load balanced and distributed)
- Is the alarm management solution E2E performance reports, benchmark reports, audit reports are available to measure the solution success, failure and integrity?
- Are the available alarm reports can identify the top ten nodes generating most number of alarms on daily basis to address them?
- Whether Business Continuity plan for each and every piece of the components involved in alarm management solution and proven disaster recovery procedures are available?
- Is the alarm trend and forecasting reports in terms of current alarms, load on systems and the alarm queue length are available?
- Alarm severity: Is it correctly mapped and reflects the true situation?
- Is the value added information to help NOC operators for faster incident resolution available?
- Are NOC operators able to map Incidents to probable Root Cause and then to the real Problem on a managed object within very short time?
- Is there a dedicated person or a team assigned with Key Performance Indicators (KPIs) to investigate the alarm trend analysis and for managing the top ten noise generating nodes / element managers?
- Is it possible to produce performance report on the NOC operators in terms of number of alarms received, acknowledged and resolved with their individual user account during their shifts to enhance the quality of service, business deliver to end customers?

With the above analysis we plotted the following radar charts to identify the areas that need immediate attention.

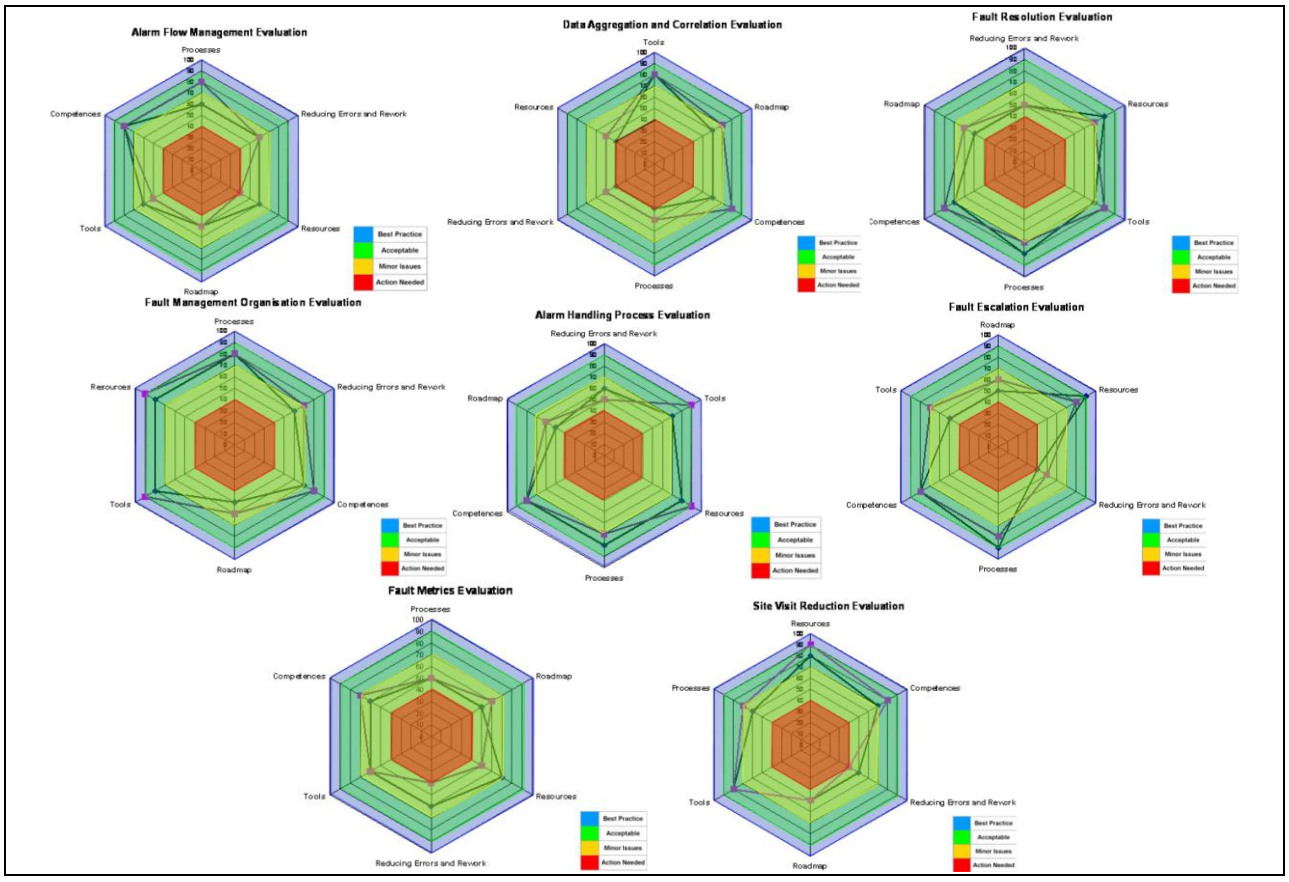


Fig. 6: Alarm Analysis Radar Charts Results.

6.5. Optimization of Alarms - Processes

Once the issues are identified an Alarm Planning Cell (APC) was established with members from different parts of the organization. The scope of the APC includes but is not limited to the following key functionalities

- Rationalization and reduction of the current types & volumes of alarms originating from each network platform.
- Review and improve Alarms management solution architecture.
- Development of design rules so future alarm management designs are optimized to enable Operations to deliver to Key performance Indicators (KPIs).
- Manage elements owners responsibilities and their interaction with the APC
- Audit, Performance and benchmark reporting
- Quality of service and customer experience
- Review and refine processes associated with Alarms Management.
- Documentation of an alarm management strategy. To cover E2E Alarm Management solution design implementation and acceptance process.

Governance and Structure was set up as below:

Frequency of meetings

- There will be weekly meetings with the APC team and the project manager will circulate the meeting minutes with actions against their timeline

- Fortnightly APC chair will meet with Project managers and Alarm Management Architect to see the progress and align with the Business goals and deliverables
- APC with their project managers will present three months, six months and 12 months action plan with SMART deliverables and their Business benefits
- Alarm management solution customers (NOC managers) and Business will be presented with alarms trend reports and the progress made on monthly basis by the project managers

Once the process is established, technology and people aspects were addressed as below

6.6. Optimization of Alarms - Technology

Master Alarm Plan is the guiding principles and targets by which the alarms are configured and measure the alarm performance. It will cover the following key criteria as a minimum to address the quality of alarms.

- what is an alarm
- How severities are set based on its impact and time to respond
- General alarm considerations covering operator assisted notes in plain English text
- Which alarm clears which other alarms and its time frame to set auto clear or correlation
- Correlation logics design with filter rules to filter consequential, derived, transient, flapping alarms and known scenarios based alarms.
- Alarm performance criteria and resolution activities

Once the alarm plan is developed and implemented, next phase is to filter the unwanted alarms to reduce the quantity of alarms [7]. Unwanted noise alarms should be controlled at the source level and if it is not feasible, they should be filtered out by using effective correlation [8] logic filters. Figure 7 shows the event correlation logic engine with timer which intercepts the flood of alarms and filter them out prior to passing or creating a new root cause event to the NOC operator.

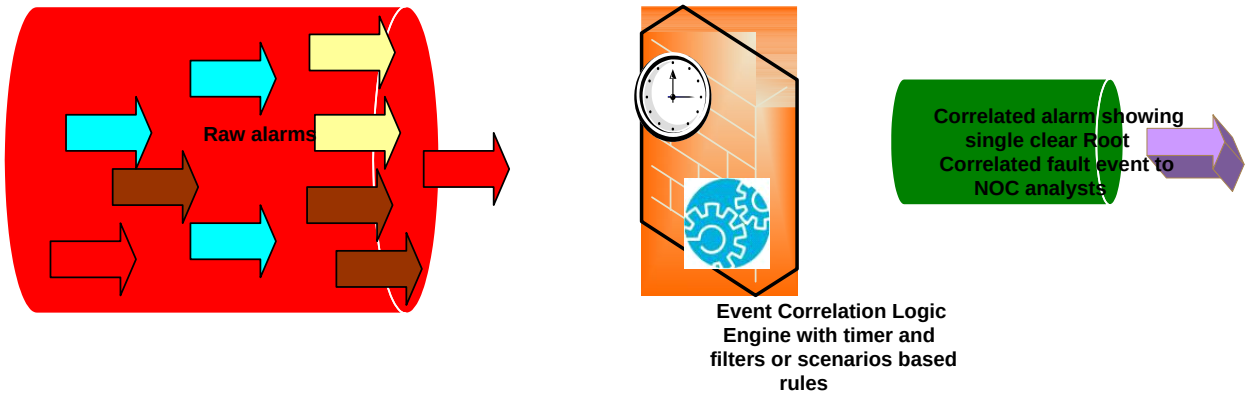


Fig. 7: Alarm Correlation Engine.

Following set of filters could be defined as applicable to the scenarios to cut down the noise alarms and reduce the quantity of alarms passing to the NOC operators.

1. Corrective filter:

A filter that can correct the event parameters such as probable cause, severity, additional information etc based on pre-configured rules for managed objects and time

Example: During nightly backups, servers send lot of performance bottleneck alarms which came with severity of high can be assigned with perceived severity of minor considering the time using corrective filter.

2. Tap filter:

A simple filter that can turn on/off the incoming events and passes or rejects them to the operator console

Example: Scheduled maintenance might generate known down/up alarms. This can be filtered through tap filter easily by setting provisioning flag for those objects undergoing scheduled maintenance.

3. Transient filter:

A time-based event filter that keeps the incoming alarms for pre-configured time (say 5 minutes) and if the condition didn't clear within that interval it passes the event to NOC operators

Example: Link saturation could cause the objects failed to respond within the set timeout period for proactive polling which will generate node down and up continuously. These can be filtered through transient filters easily with set time period for clear alarms. If the clear alarm didn't come within the set time period, it will pass the critical event to operators.

4. Threshold filter:

An event will be passed if the threshold is crossed within set timeframe

Example: Servers might send high CPU utilization for peak utilization which lasts for a short while but the event will be passed to operators if the threshold had breached and last for set time period.

5. Heap filter:

This filter collects and queues the alarms for set time period. Once the time is expired a new alarm will be passed to operators with additional information.

Example: In a service provider environment when an application server goes down, it may generate alarms from switch, load balancer, firewall, and the server itself. If we know the scenario, heap filter can be used to collect events and look for certain parameters to see the alarms from switch, load balancer, firewall, application server in a set time interval and generate a new alarm with combined value-added information.

6. Toggling filter:

An event will be passed to the NOC operator only if there is no context or after the set time period.

Example: If a switch or router is managed it is not uncommon to see interface flapping alarms whenever the object is restarted which will fill up the NOC operators screen with Node down, Interface down and Interface Up and node up alarms. In this scenario toggling filter can be used to suppress all interfaces down and up alarms if there is an associated node down and node up alarm within set time period.

A single filter or a combination of filters may be applied in series with the following order of precedence.

Corrective ➔Tap ➔ Transient ➔ Threshold ➔ Heap ➔ Toggling

The attributes of raw alarms that can be used in filters design include Managed object, Alarm Type, Alarm Time, Severity, Notification identifier, Source identifier, Probable cause, Alarm text, Managed object status, Trend indication, Alarm cause, Outage flag and Alarm specific message key.

6.7. Optimization of Alarms - People

The flood of alarms is due to mis-configuration of alarm platforms and lack of correlation circuits and intelligent filters to combine all consequential and derived alarms to a single root cause alarm with right severity. There was no accountability in terms of ownership to deliver the E2E solution and to achieve business vision. To address these issues on the alarm platforms, it was recommended to have a dedicated team of people who will look after the alarm systems in terms of its design, implementation, remediation, upgrades and reporting. APC members include Project manager, Alarm Architect, NMS Technical Specialist, NOC Operations Team Leader, Managed elements technology specialist and Vendor

representative.

It is very important to train the operators and get them certified against vendor certifications to ensure they are able to use the management software features. To close the loop they can send their feedback when they find alarm patterns during certain incident, which can be used by the engineering team to develop scenarios based filters.

Benchmark the alarm performance with the introduced changes and trend information. This will be critical in getting Business buy-in for further improvements and setting up a Continuous improvement Program.

6.8. Continuous improvement program

Implementing Continuous Improvement Program (CIP) through APC carried out the following tasks

- Monitor the alarm occurrences trend
- Analyze the possible causes of the alarm (legitimate, spurious and redundant) trend
- Fine-tune the alarm settings and update Master Alarm Plan
- Develop additional filters and smart actions to diagnose the alarms
- Develop additional reports showing the impact of the recently introduced changes
- Update Master Alarm Plan, alarm solution architecture and design documents as per Business growth and requirements and publish them in a web server which will be accessible based on users' access role.
- Measure the success and broadcast to the Business through regular communiqu é

6.9. Results of Alarms Optimization

The alarm rate has dropped from 70/minute to 0.05/minute which has vastly improved the operator effectiveness and usage of systems resources.

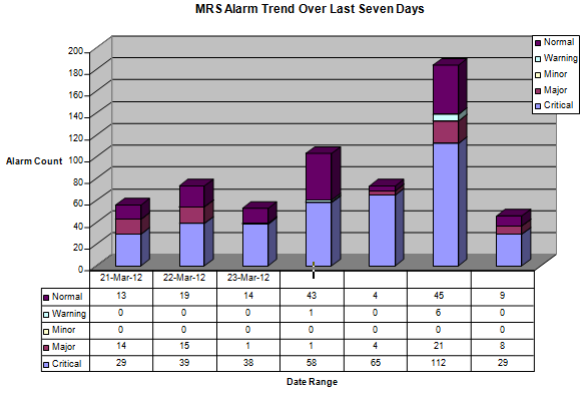


Fig. 8: Alarm Analysis Graph results after optimisation.

With the reduced alarm rate NOC operators were able to manage alarms through a single Manager-Of-Manager alarm console instead of multiple alarm consoles. Noise alarms were filtered at source level or at their element managers prior to pass them to centralized alarm console using the following umbrella model features of informing delay, Filtering and correlation at various levels.

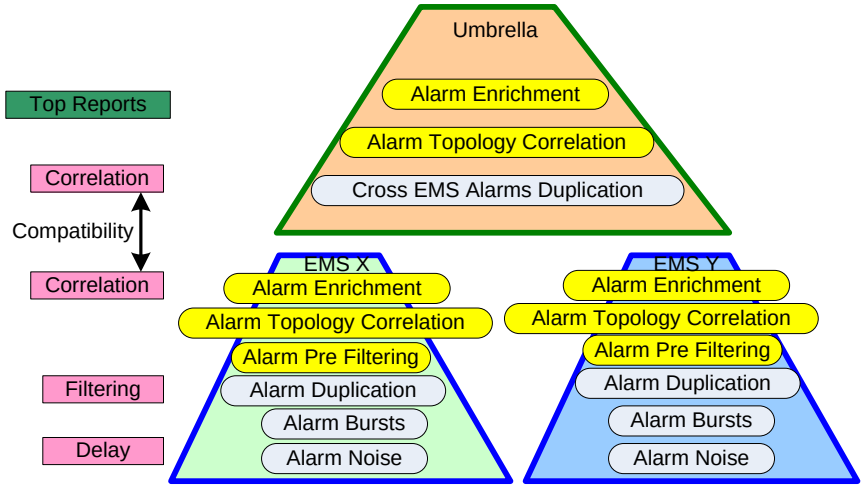


Fig. 9: Alarms Optimisation Strategic Approach.

7. Conclusion

Advances in technology and increases in customer demands, government regulation have jointly made alarm management more important and more difficult. Alarm management is not just about reducing alarms; it is about responsible network management and increasing network reliability and uptime. Alarm management is just a good process for managing and protecting revenue generating network reliability and uptime. Implementing effective alarm management is not a do-it-yourself job but a highly technical subject which needs a good understanding of technologies, customer requirements, and topology information to understand what to manage and how often to proactively poll to manage, architecture, SLA, business process challenges and list of stake holders and developing effective correlation logic filters. An inadequate alarm management solution can cripple the reliability of the network, increased misuse of resources and equipments failure, reduce the value of products and services business offer to customers, reduce the business reputation in the market which in turn will increase the customers churn and revenue loss to Business.

8. References

1. Aidarous S & Plevyak, T. (1994), Telecommunications Network management into the 21st century, 1st edition, IEEE press.
2. Bob B. (2003), 3 fatal mistakes in managing alarms in your communications and data networks and how you can avoid them, 2003 (available whitepaper from http://www.dpstele.com/white-papers/)
3. Díaz S, Escudero JI & Luque J (2000), Expert system-based alarm management in communication networks, ICEIS.
4. Gould, J. (2003), Institutionalizing alarm management, (white paper available from http://www.automation.com/resources-tools/articles-white-papers/manufacturing-intelligence-industrial-information-management/institutionalizing-alarm-management)
5. HP openview TeMIP Event filtering and correlation software reference manual (2004), Hewlett Packard.
6. Thirumalainambi M. (2003), Tuning NNM servers, Journal of SysAdmin, Nov 2003.
7. Todd R. (2006), Network alarm monitoring fundamentals,(available whitepaper from http://www.dpstele.com/white-papers/)

8. Tony B., Peter G.,Jacqueline M., Guilherme P., Michael W. (2004), Event Management Best Practices, IBM Redbooks, SG24-6094-00, June 2004.
9. William S. (2003), Network management, IEEE computer society press.

About the Authors

Thirumalainambi Murugesh received his Ph.D. degree in Electrical & Electronic Engineering specializing Managing Networks and Internet Security from the University of Auckland, New Zealand. He has been working in the ICT Carrier and Service provider industries over the last 17 years in Solution Architecture, Design, Implementation, and Management of resilient networks, high-performance Unix computing systems and applications focusing on reliability, redundancy, and security. He can be reached at Thirumalainambi.murugesh@au1.ibm.com.

Chandrasekara A.S. Aiyer leads the Corporate Architecture team at IBM , Australia. He has been involved in the research and development over last ten years in terms of developing reference architecture for Enterprise Networks Systems management and Cloud Computing. He can be reached at aiyerch@au1.ibm.com.