Network Dependability Monitoring through Statistical Analysis of Alarms

Jorge Moreira de Souza e Simone Schmidt

***Resumo*— Este artigo mostra como técnicas estatísticas simples podem ser usadas na análise do enorme fluxo de alarmes gerado diariamente em uma rede de Telecomunicaçãoes de modo a identificar pontos fora-de-conrole que ajudam a dirigir a atenção do gerente de rede para o foco do problema. O principal objetivo é equipar o gerente de rede com técnicas e ferramentas que permitam a análise com facilidade e rapidez do fluxo de alarmes permitindo o planejamento e execução de ações preventivas.**

***Palavras-Chave* – Gerência de alarmes, Redes de Telecomunicações, Confiabilidade, Estatística, Gráficos de Controle, Análise de Tendência.**

***Abstract* – This article shows how simple statistical techniques can be employed in the analysis of the alarm flood that is daily generated in a Telecommunication network helping the manager through the analysis of out-of-control points in identifying the root cause. The main objective is to provide to the manager a set of techniques and tools allowing an easy and fast analysis of the alarm flood guiding the planning and execution of preventive actions.**

***Keywords* – Alarm Management, Telecommunication Network, Reliability, Statistical techniques, Control Charts, Trend Analysis.**

I. INTRODUCTION

The telecommunication networks are providing more and more different services for the users. Services increasing also contribute to an increase in network complexity affecting operation and maintenance. An additional challenge is the high dependability required for the services as many activities like commerce, health, banking, etc rely on the correct and sustainable functioning of the network.

To attain the required dependability techniques such as fault-tolerant design and testing [1], software reliability [2] are employed during development and deployment to derive metrics and models to quantify and validate the proposed network dependability.

Although the network may have the necessary design for high dependability its sustainable functioning relies on a daily operation and maintenance activities analyzing and fixing alarms and faults some of them very critical leading to network unavailability if not fixed in time.

In the context of network operation and maintenance Fault Management is of paramount importance to achieve the required level of dependability. In current network management systems the operator is overloaded by the flood of alarms generated by equipments and protocols from very different parts of the network.

Processing the alarm flood is a difficult task due to:

- The network complexity combining different network elements and services generating a multitude of faults scenarios;
- The burst characteristic of alarm occurrences. Besides the severity classification and some filtering of transient anomalies, the operator is faced with a lot of alarms and should decide for intervention in a short time;
- The technology evolution requiring the addition of new elements and services to keep pace with user needs.

The current published works on Fault Management can be divided into three interdependent solutions:

- Alarm filtering/reduction looking at primary alarms identification (filtering out non important secondary alarms) by this way reducing the alarm flood [3],
- Root cause analysis aiming at identifying the possible causes based on the primary alarms scenario [4-5],
- Retrieval of useful fault patterns based on statistical analysis of daily alarm logs [6].

They are interdependent in the sense all of them provide information for knowledge discovery of fault manifestation.

This paper deals with the third bullet showing some simple statistical techniques that helps the managers in analyzing network alarm anomalies before possible catastrophic manifestation by deciphering the alarm flood searching for abnormal events (out-of control points) and identifying the possible origins.

In the following section it is explained the main ideas behind the use of statistics for network management. Section III covers briefly the expression used for control chart evaluation and trend analysis. To show the power of

Jorge Moreira de Souza and Simone Schmidt are System Engineer at FITec, Fundação para Inovações Tecnológicas, Campinas, SP, Brasil, E-mails: jmdsouza@fitec.org.br, sschmidt@fitec.org.br.

the techniques, in section IV a real alarm log is used to flag critical situations before their occurrence.

II. ALARM LOGGING AND MONITORING

Alarm monitoring is provided online to the operator at the Network Management Centre. Alarms are collected and displayed for operator with indications like:

- Date and time the alarm has been activated,
- Date and time the alarm has been deactivated,
- Network Element that generated the alarm,
- The consequence in the network (link loss, signal loss, synchronization loss, high error rate, etc.),
- Warnings (upper or lower limits to monitor resources availability or out of specification levels),
- Alarm severity (critical, major, minor, etc),
- Others.

An alarm does not necessarily mean a system failure. They are introduced to warn abnormal conditions related to the network elements, links, protocols, etc. that may lead to network and/or service crash if the correct maintenance action sequence is not provided in time.

How the statistical analysis of alarms can lead to a more dependable network and service? The rationale behind is that:

- The system has a "sunny" behavior characterized by an average and variance of the alarm flood for elements considered as similar,
- Generally the change from "sunny" to "rainy" behavior is not abrupt but preceded by warning alarms pointing out to functional deterioration in the system,
- This deterioration produces a change in the "sunny" average and variance of the alarm flood,
- Upper and lower limits can be evaluated for these changes pointing out-of-control points when exceeded,
- A preventive action upon the out-of-control points may prevent a critical situation that may affect the network dependability.

In [6] early warning of failures based on alarm data is raised by analyzing the data following three principles: overall counts of alarms, Pareto distribution by sub-units as a signature of normalcy, and clustering of alarms that are typical to a failure mechanism.

The approach proposed in this paper uses two statistical tools to start preventive analysis and possible maintenance actions:

- Control chart techniques very used in manufacturing and software quality control [7-8] to flag out-of-control points that may be: a given day or period, a network element, etc.,
- Trend analysis to flag an alarm increase rate beyond a specified level.

III. STATISTICAL TOOLS

A. Control charts

For a stable system the failure/alarm rate should be within controlled limits along the period. This is expected for system under system test or already delivered. The out-of-control points may be caused by abnormal system utilization, a feature weakly integrated with abnormal failure behavior, lack of resources, software aging, etc.

The objective of control charts in process control is to detect the occurrence of assignable causes of process shifts to take necessary corrective actions. This tool can be used in our context to validate the collected failure data against the assumptions and to detect possible weak points in the network operation.

The idea behind the control charts is that a process displays variation when measured over time or a set of items and hence it is possible to categorize the sources of variation as follow:

- Variation due to phenomena that are natural to the process,
- Out-of-control variations that have assignable causes that could be prevented.

The area of opportunity for the occurrence of alarms depends on the sample size/period, i.e., a day, a week, etc. In telecommunication network a practical observation is that the alarm rate also increases with the traffic. In this case the area of opportunity should be the traffic variation along the day, for example.

For the sample *i* let *n(i)* be the number of alarms with area of opportunity *u(i)*. The average number of alarms is *n(i)/u(i).*

Consider that *n(i)* is a Poisson variable. The parameters of the control chart are:

$$UCLi(LCLi) = \bar{u} + (-)3\sqrt{\frac{\bar{u}}{u(i)}}$$

$$CL = \bar{u} \qquad (1)$$

where

$$\bar{u} = \frac{\sum n(i)}{\sum u(i)}$$

The control chart has a ***centerline*** (CL) and ***upper control*** (UCL) and ***lower control*** (LCL) limits. Measurements are plotted on the chart versus a time line or inspection units. Measurements that are outside the limits are considered to be out of control.

If the process is in control the ***centerline*** value can be used as an estimate of the failure/alarm rate.

In this paper the alarm data is collected daily and the area of opportunity is constant and equal to one day period.

B. Trend analysis

Out-of-control points represent a departure from stability measured by a departure from the average behavior. When it is detected the abnormal alarm condition has already occurred. In many cases this abnormal alarm condition is preceded by an increase in the overall alarm rate changing the "sunny" scenario of no statistically significant trend to a trend increase or decrease.

In this paper two statistical trend analysis tools are used: moving average and Laplace trend analysis. Moving average is widely used and generally available in spreadsheet tools for data analysis.

Laplace trend analysis is very used in software reliability analysis to detect reliability growth/decay from the exponential model [9].

Let

k be the time period

n(i) be the number of observed alarms during the time period i

y(i) cumulative number of observed alarms up to period i

p number of time periods during the observation period

u(k) Laplace trend factor at time period k of the series of events n(i)

The factor u(k) is [see 10 for the mathematical derivation]:

$$u(k) = \frac{\frac{\sum_{i=1}^{k}(i-1)n(i)}{y(k)} - \frac{k-1}{2}}{\sqrt{\frac{k^2-1}{12y(k)}}}, k = 2,..., p \qquad (2)$$

1. u(k) oscillation in the interval [-2, +2] suggests no particular trend,
2. Positive values of the trend factor *u(k)* (> 2) suggest a reliability decay in the observed time period,
3. Negative values of the trend factor *u(k)* (< -2) suggest a reliability growth in the observed time period

IV. Alarm analysis using the statistical tools

Before applying the statistical analysis the network must be analyzed for clustering of network elements. A cluster is formed by the network elements that are expected to have similar failure behavior. This clustering depends on the element hierarchy in the network, function, capacity, environment, reliability, etc. Each cluster is monitored separately.

The following steps are necessary before analysis:

1. Identify clusters of network elements;
2. Define a window observation period for which the analysis is carried out;
3. Monitor all the network and clusters alarms for out-of-control points and tendency changes;

Using the statistical tools the network manager is able, among other possibilities, to focus on:

1. The overall alarm behavior over the observation window quickly identifying the out-of-control point and the day of occurrence;
2. Idem for the alarm behavior per severity;
3. The alarm distribution per network element at the day of an out-of-control occurrence;
4. The trend in alarm behavior;
5. Etc.

One of the values for the manager of having a broad analysis possibility is tailoring the analysis sequence based on the processed alarm information. A future objective is to specify and implement a friendly tool allowing an easy navigation over the processed alarm information.

To illustrate some analysis possibilities a real situation is exemplified in the sequence. This is a posteriori analysis using the statistical tool to flag critical situations that could be written differently if the alarm analysis were available.

The alarm log used was collected from a network in operation. Their severity is informed and classified as critical, major and minor.

A. An out-of-control situation

The window observation period is 31 days, all the alarms are monitored, there is just one cluster, and there are 37 network elements.

Two out-of-control points occurred in period 23 and 24 (see figure 1).

At period 23 a flood of minor severity alarms in its majority appeared in the screen. Going over the analysis per network element it is possible to identify the region of the network they came from and work proactively (see figure 2).

In this example the next period (period 24) is also an out-of-control point of major alarms. Could this situation be avoided based on the information of the previous period?

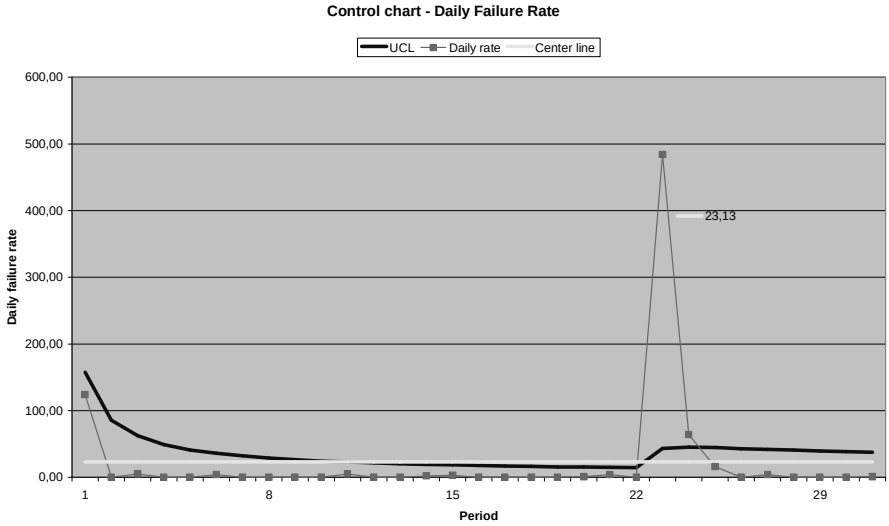

Fig. 1 A punctual out-of control situation

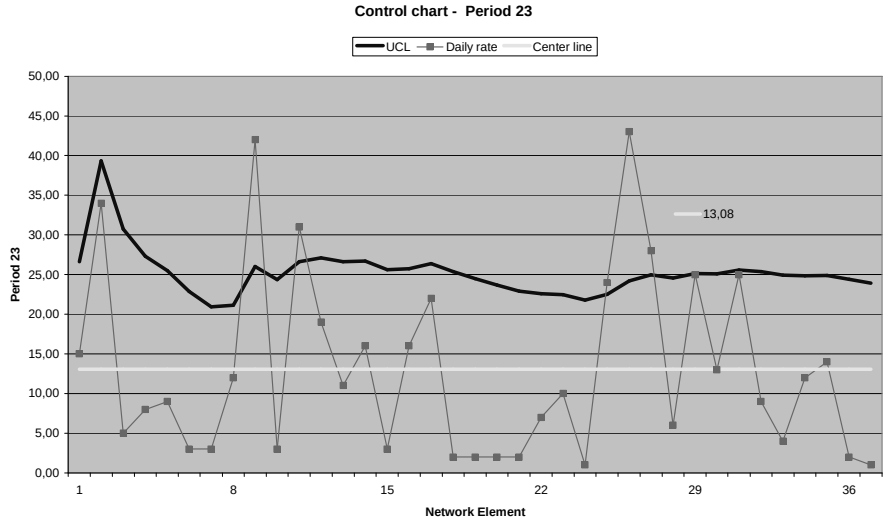

Fig. 2 Alarm behavior per network element at period 23

B. Alarm trend increase

The same network is analyzed now over a different window observation period (see figure 3).

The alarm behavior shows a consistent out-of-control tendency after the period 15. The moving average evaluated over 10 days also shows this tendency.

A more emphatic result is obtained using the Laplace trend (see figure 4) that is evaluated over the observation period. It indicates that the tendency to increase is sustained over the period suggesting that something went wrong.

In this case after period 31 there is a critical occurrence with many links down over the network.

V. Conclusions

Alarm/Fault Management is of paramount importance to maintain the availability of Telecommunication network.

The network managers are daily faced with a flood of alarms that according to their severity and online analysis drive the maintenance actions.

The use of statistical tools can help in this analysis identifying to the manager the abnormal behavior and providing the search facilities in order to identify the root causes so a preventive action can be planned and executed avoiding a possible network catastrophic state.

Through a posteriori analysis of some alarm data of real situations this analysis proved valuable and encourages the availability of a tool allowing a quick search and analysis of out-of-control points per network attributes.

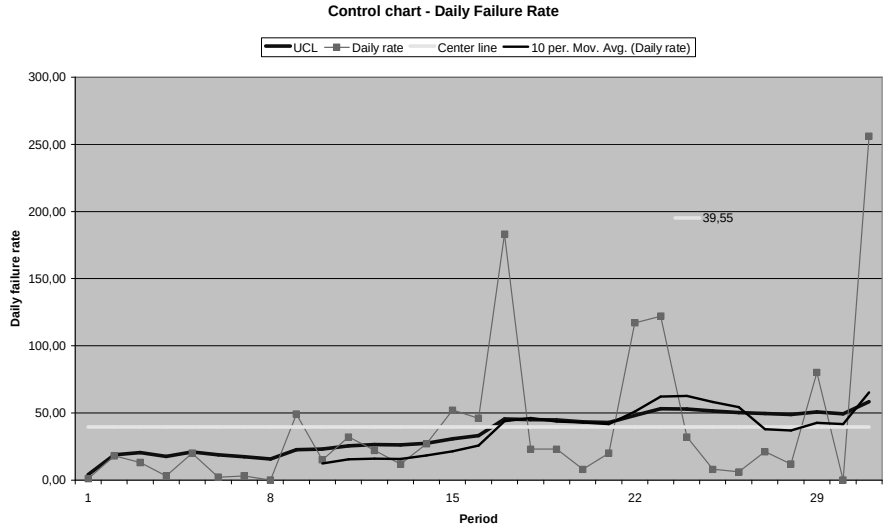

Fig. 3 A window observation period with increasing trend in alarm manifestation.

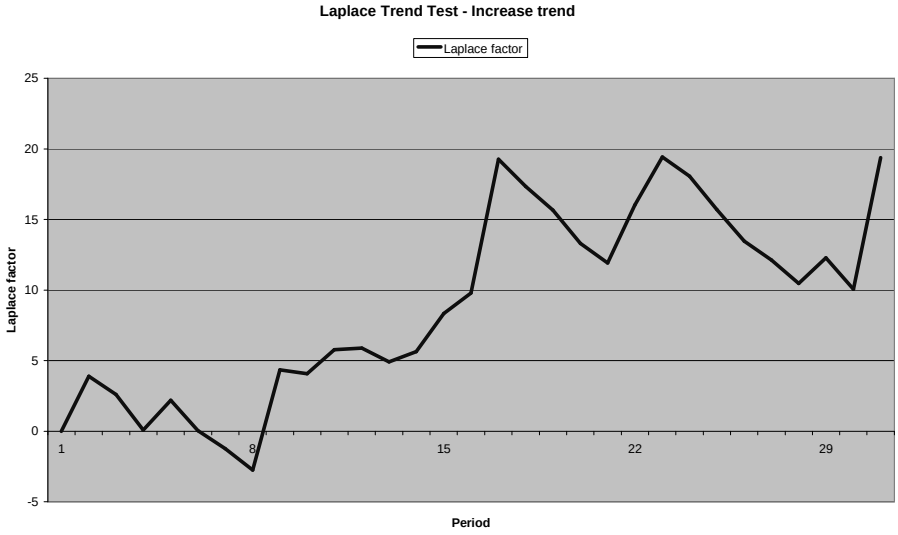

Fig. 4 Laplace trend analysis

References

[1] See IEEE Fault-Tolerant Computing Symposium, and Brazilian Workshop on Fault Tolerance.

[2] J.D. Musa, *Software Reliability Engineering*, McGraw-Hill, 1999.

[3] J. Tuszynski et all, "A Pilot Project on Alarm Reduction and Presentation Based on Multilevel Flow Models", *Proc. Enlarged Halden Programme*, Norway, 2002.

[4] A. Hanemann, M. Sailer, D. Schmitz, "Assured Service Quality by Improved Fault Management", *ICSOC 2004*, New York, USA, Nov 15-19, 2004.

[5] M. Garofalakis, R. Rastogi, "Data Mining meets Netwok Management", *DMKD Workshop*, CA, USA, May 20th, 2001.

[6] D. Levy D., R. Chillarege, "Early Warning of Failures through Alarm Analysis – A Case Study in Telecom Voice Mail System", *IEEE Int. Symp. Software Reliability Engineering* (*ISSRE 2003*), Denver, USA, Nov 17-20, 2003.

[7] D.C. Montgomery, *Introduction to Statistical Quality Control*, J.Wiley, 1997.

[8] W.A. Florac, A.D. Carleton, *Measuring the Software Process*, SEI Series on Software Engineering, Addison Wesley, 1999.

[9] J.D. Musa, A. Iannino,K. Okumoto, *Software Reliability – Measurement, Prediction , Application*, McGraw-Hill, 1987.

[10] M.R.B. Martini, K. Kanoun, J.M. de Souza, "Software-Reliability Evaluation of the TROPICO-R Switching System", *IEEE Trans Rel*, VOL 39, NO.3, Aug. 1990.