SAFE Tool for Avoiding IT Infrastructure Service Outages and Degradation of Service

Raman Swaminathan, Jambhu Kumar, Venkatakrishnan, Dr. Selvan C
Delivery Excellence and Analytics Lead, Integrated Delivery Leader, Principal Data Scientist, Global Europe
Delivery Excellence (Quality) Leader, Nordics, IBM India Pvt Ltd, Chennai, India

Abstract

Future Incidents Avoidance Solution (SAFE) is built to analyze and detect an early problem for application, middleware or infrastructure problems before they impact service. The software helps you avoid outages and increase service performance. In this paper we propose a predictive model called SAFE tool which turns terabytes of big operational data into understandable and actionable insights for quicker problem solving and better overall service.

Keywords – *SAFE, MARCC, MTTR, MTBF, Infrastructure Service Outages, Degradation of Service*

I. BACKGROUND

Today in IT we monitor and resolve IT issues and react to incidents and events. This is no longer enough, we need to be proactive and prevent incidents and customer impacting outages. Rather than reducing the MTTR (Mean Time To Resolve), we need to anticipate and prevent application degradations and service outages – Predict incidents before they become service impacting (Mean Time Before Failure - MTBF). SAFE uses algorithms patterns and behavioral learning for data analysis, to understand how applications and their infrastructure should normally behave and interact. It establishes baselines for normal behavior, adapts to changes within the environment and issues alerts on detected anomalous behavior. This gives operational teams a critical tool to detect trends and forecast future issues through the automatic analysis of data. Thus, reducing the amount of effort required to identify the root cause of application degradation and spending time prior to service impact on resolving potential issues rather before these translate into incidents. The worst thing that can happen to any IT Infrastructure industry is performance degradation. Whether it's a failed transaction or a full blown outage, downtime costs money, not to mention customer loyalty. IT industries are now looking for ways to gain insight into issues before they impact end users.

II. INTRODUCTION

What is Future Incidents Avoidance Solution?

SAFE is a tool which identifies potential incidents before traditional monitoring or operations knows to look for them by self-learning the normal operational behavior of the dynamic infrastructure. It can analyze performance and monitoring data across silos, domains and vendors, providing a single analytic solution for complete heterogeneous monitoring of infrastructure. There is no complex manual intervention required for setup and the machine-learning algorithms provide meaningful early warning alerts. Future Incidents Avoidance Solution provides early warning of abnormal behavior which might be indicative of potential outage, service degradation or unexpected change. It dynamically builds thresholds and baselines without need for configuration.

Future Incidents Avoidance Solutionworks through a series of algorithms using domain knowledge to perform Data insights to provide:

I. **Early detection of problems** to avoid service impacting problems. Future Incidents Avoidance Solution has multiple algorithms that learn normal behaviour and alert when that behaviour changes significantly giving a user the time to determine the cause of the change, and why, and take the necessary action.

II. **Insight through automatically discovered mathematical relationships**, which are shown to help identify the root cause of a problem. Metrics are related because they have been discovered to be:

   a. Granger Causing, e.g. the number of users accessing a web page and the load on the database server feeding the web page

   b. Related Event - shown to be historically anomalous around the same time. (e.g. when a key piece of core infrastructure has problems, and then all the other parts of the infrastructure

have problems – but otherwise not related to each other)

c. Correlated - e.g. the load on a group of application servers as people login to them at the start of the working day

III. **Dynamic thresholds** or baselines are automatically built by Future Incidents Avoidance Solution by determining what is normal at every analysed period, such that: e.g. If backup does not occur at its regularly scheduled time, Future Incidents Avoidance Solution will alert. Similarly, the scheduled backups, there will be no anomaly informing of high Disk activity during the backup. This is already understood, so Future Incidents Avoidance Solution does not flag this. Future Incidents Avoidance Solution' adaptive seasonal baseline provides highly effective baseline anomalies. Noise is reduced when compared to traditional thresholding systems.

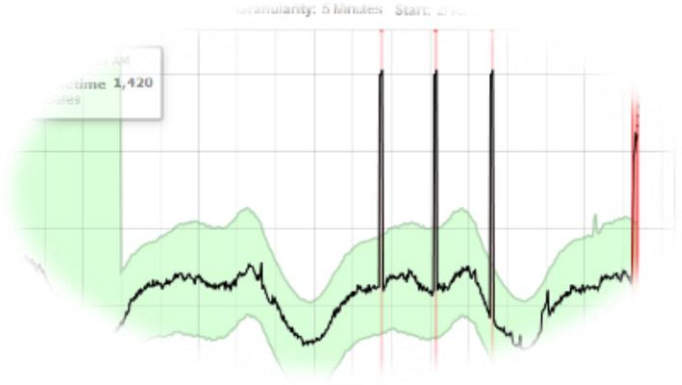

Fig. 1 Anomalies reporting system

IV. **Forecasting** feature of Future Incidents Avoidance Solution predicts show a metric value will change over the coming time periods and thus allow you to prioritize the set anomalies raised by Future Incidents Avoidance Solution.

What is an Anomaly?

An anomaly is when a KPI which deviates from its normal behavior. Future Incidents Avoidance Solution learns, defines and refines normal behavior during training. An anomaly may be temporary. The scale of an anomaly is based on a model of expected behavior which is learnt and not defined. The observation is scored with how likely the observation does not come from the model. SAFE tests every model before it is used and does so automatically to ensure that it does not underfit or overfit the models. This is to avoid false positives. The SAFE threshold moves with the data and creates a dynamic model.

What do differently type of Anomaly's denote?

- Brown – This means a single anomaly occurred on a node. There is a deviation of one metric on one resource.
- Orange – This means multiple anomalous metrics on the same node or across multiple nodes.
- Red – This usually means there is some issue with the collection itself (no data from node, the application is unhealthy, etc.).
- Pink– This is informational. These messages usually SAFE related system information and are checked by the admin team and we do not need to react to it.

III. MARCC MODEL

SAFE tool uses MARCC model for early detection of anomalies.

1) **Monitor: -** Monitoring SAFE tool helps us tospot problems anywhere in your infrastructure, so that we can rapidly identify their causes and minimize service degradation and disruption.

2) **Analyze: -** SAFE toolanalyses for any deviations from the KPI and throws an Alarm which needs to be investigated. Analysis discovers the root cause e.g. application or extraordinary job has caused a change in behavior and it is expected to normalize. Baseline must be confirmed as normalized once the root cause is determined.

3) **Report: -** All the anomaly's received for each and every hour would be reported with necessary stakeholders in the form of a dashboard.

4) **Collaborations and Classification: -** Technical Collaboration is done between the Client SME and Service provider SME to classify these anomaly's into Brown, Orange, Red and Pink anomaly's.

5) **Action taken: -** Based on the anomaly classification, technician would take proactive

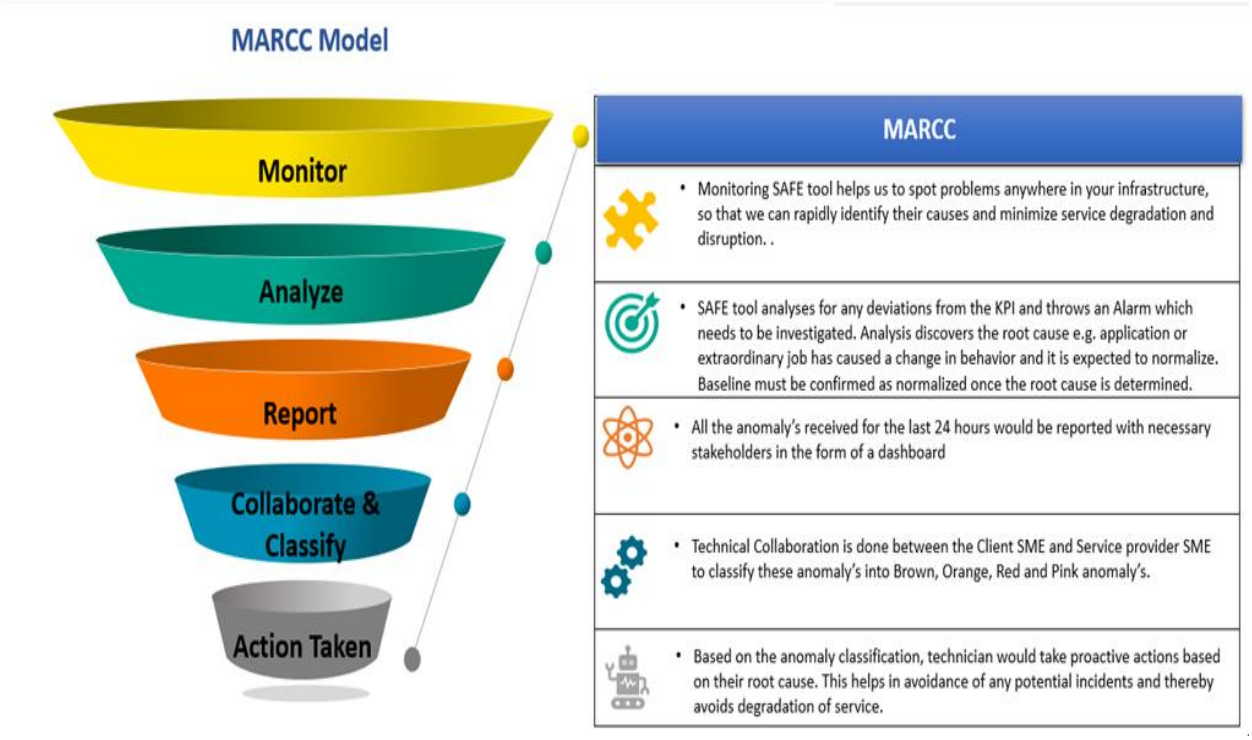

Fig. 2 MARCC model

I. PROCESS FLOW

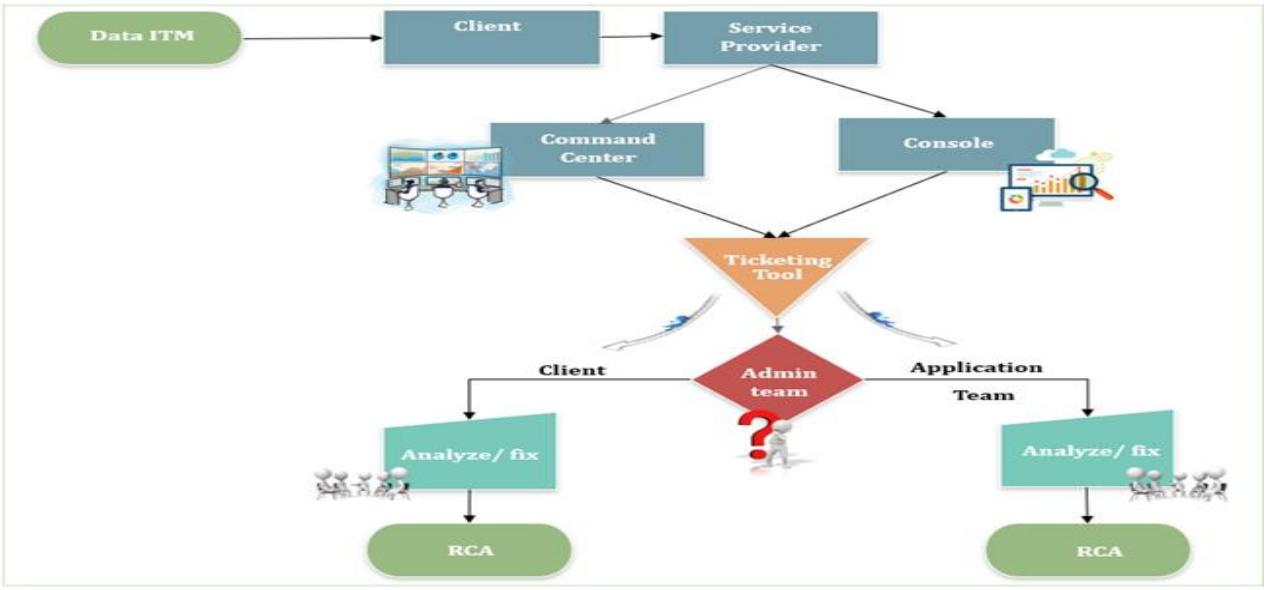

Fig. 3 Process Flow – MARCC Model

IV. BENEFITS

Gaining insights into negative trends and anomalies in your IT Service Management environment and infrastructure makes it easy to take proactive steps to:

- Reduce Operational Costs
- Increase Mean time between Failures
- Avoid Service Outages
- Improve Operational Efficiency

V. BUSINESS VALUE

The current implementations for automation and analytics are to provide supporting arguments for long term investment for Information technology Infrastructure Industry, that these can be used to manage daily operations and result in better quality of end-user experience.

- Move away from operational incidents to increased service
- Set a course for maturing the analytic tools and incorporating them into business plans
- Show business value of these tools
- Holistic dashboards for swift business decisions by stakeholders
- Define strategy aligned with the overall landscape for the client
- Identify impact on the Operational Model (structural, skills, automated and manual interventions across different managed environments, Authentication & Authorization etc.)

VI. CONCLUSION AND FUTURE PLANS

In today's scenario most of the clients demand availability of their critical IT system 24 by 7. One of the most important benefits of the SAFE is the ability to forecast system alert in advance. This has a great implication on the avoidance of degradation of the IT service.

Before adoption of a technology like Future Incidents Avoidance Solution, we need to first change the inherent mindsets of system administrators on handling of incident management and a reaction to incidents. For many years we have all worked with incident management, reacting to an incident after the failure has occurred, and then analyzing and correcting the issues, and spending many hours working to find the root cause following system recovery. The need to pre-empt the failure and determine the cause for a change in the behavior, before there may be any indication of an issue on the server. Here there is a need to throw away the thought of incident and resolution and look to at the root cause analysis before an incident occurs. We need to ask ourselves: Why? Why has SAFE suddenly identified a behavioral change, why did this occur? we can apply the 5 Whys, to an anomaly and work to determine how that anomaly could potentially lead to an incident.

In future we envision to build Analytics with this tool which would help in providing meaningful insights to the stakeholders to take swift Business decisions.

REFERENCES

[1] Z. Gong, X. Gu, and J. Wilkes. Press: Predictive elastic resource scaling for cloud systems. In Network and Service Management (CNSM), 2010 International Conference on, pages 9–16. IEEE, 2010.

[2] Muzammil H Mohammed,Faiz Baothman,"Intelligent Workload Management of Computing Resource Allocation For Mobile Cloud Computing",International Journal of Computer & Organization Trends (IJCOT),Volume - 5 Issue - 2,2015.

[3] X. Gu and H. Wang. Online anomaly prediction for robust cluster systems. In Data Engineering, 2009. ICDE'09. IEEE 25th International Conference on, pages 1000–1011. IEEE, 2009

[4] G. Jai Arul Jose, C. Sajeev,"Implementation of Data Security in Cloud Computing",International Journal of P2P Network Trends and Technology (IJPTT),Volume-1 Issue-1,2011.

[5] F. Salfner, M. Schieschke, and M. Malek, "Predicting failures of computer systems: a case study for a telecommunication system," in Proc.of IPDPS, 2006

[6] [4] P.H.S. Teixeira, R.G. Clemente, R.A. Kaiser, and D.A. Vieira Jr. Holmes: an event-driven solution to monitor data centers through continuous queries and machine learning. In Proceedings of the Fourth ACM International Conference on Distributed Event-Based Systems, pages 216–221. ACM, 2010.

[7] [5] Z. Gong, X. Gu, and J. Wilkes. Press: Predictive elastic resource scaling for cloud systems. In Network and Service Management (CNSM), 2010 International Conference on, pages 9–16. IEEE, 2010.