International Civil Aviation Organization
South American Regional Office
Twenty Fourth Workshop/Meeting of the ICAO SAM Implementation Group (SAM/IG/24) – Regional Project RLA/06/901
(Lima, Peru, 4 to 8 November 2019)

SAM/IG/24-IP/4.1
10/31/2019

Agenda Item 4: **Assessment of operational requirements to determine the implementation of improvements in communications, navigation and surveillance (CNS) capabilities for operations in route and terminal area**

ATN IN BRAZIL (ATN-BR)

(Prepared by Frequentis)

SUMMARY

This working paper presents the implementation of the National Management Solution in the ATN-Br project in Brazil, as well as describe the solution and its technical aspects as implemented by Frequentis.

Reference:

- SAM/IG/23 Final report;

1. Background

1.1 Today the System Management landscape is composed of many independent Management Systems that are specific for every subsystem. There is hardly any information exchange between them. Regional and National Resource planning and Monitoring is a difficult and time-consuming task with this setup.

1.2 To meet the future challenges, it is important to have an integrated solution that combines and correlates the information of all subsystems of the Brazilian Air Traffic Network. With a homogenous picture of all aspects of the system far better results in terms of performance, costs and resource planning can be achieved.

1.3 A mission critical situation can easily be detected and mitigated immediately. The national management solution addresses the following operational needs identified together with the customer:

- Integration of Regional with Central National Management;
- Clear Separation of Regional and National Management Responsibility;
- High Availability by Autonomous Regional Management systems that are loosely coupled with the National Management System;
- Centralized User and Access Management;

- Situational Awareness of System Status and Transport Network for Contingency Reconfiguration and Zone redefinition;
- Ability to resume regional management in the Central Management Location;
- Integration of all Subsystem including the Data and VSAT solution; and
- Operational guidance through the daily operation processes.

1.4 The main goal is to accomplish a homogenous solution across all areas and subsystems. This will reduce operational costs and improve the situational awareness for stakeholders

2. **Analysis**

2.1 The status of many subsystems needs to be collected to form the big pictures. This takes time and management has not always the right information by hand when it is most needed. The national management system addresses that problem and provides situational awareness to the different stakeholders on different levels of the organization.

- Each Region has an independent Monitoring Elements.
  - It is fully redundant and guarantees independence when disconnected from the other regions and/or the National Center.
  - Information is distributed by using the entire Brazilian ATN Network Infrastructure (MPLS, TDM, VSAT)
- Failure Blueprints to categorize Faults / Information
  - Classifier / Product Name / Organisation etc.
  - Failure Severity.
  - Failure Information.
  - Failure Correlation.
- Failure Monitoring
  - All IT and Network equipment is monitored.
  - VCX-IP, VSAT and TDM gateways as well as CPE routers are monitored.
  - Failures are aggregated to save bandwidth on the WAN.
  - Fault information is buffered in case of network connection is lost.
- Network Performance Monitoring
  - SLA monitoring of the bearer network.
  - All aspects of the network are monitored (e.g.: Bandwidth, Delay, Packet Loss etc.).
  - Downtimes and Network availability analyses.
  - Baseline for network configuration changes and equipment replacement planning.
- Network Traffic Analyses
  - Network traffic can be analysed based on links, network segments etc.
  - QoS analyses based on Traffic classes and type of application.
  - Many other reports to support network reconfiguration and planning.
- Service Performance Monitoring
  - Air traffic management communication services (like: VHF/UHF channels, RADAR streams, data applications) are monitored end-to-end (from remote site to center site)

- Dashboards to present “per FIR” views of the operational states of the ATM communication services, as well as the underlying network asses
- ATM communication services KPIs are reported into SLA reports

- Configuration Management
  - Consistency checks between subsystem for predefined rules.
  - Compliance checks if guidelines are followed.
- Security Monitoring
  - Security appliances are monitored.
  - Reporting of malicious behavior.

2.2 The Network Management Hierarchy is an important aspect of this solution. It is driven by geographical and organizational requirements:

- Primary NMC: The National Management Center (NMC – located at DTCEATM-RJ, Rio de Janeiro) is responsible for planning and monitoring of the national air space. It needs to have the big picture about the situation in all ACC Areas. There is also a Customer Umbrella management system integrating all subsystems. The NMC provides a Northbound Interface (NBI).

- Standby NMC (Located at PAME-RJ, Rio de Janeiro): The NMC functionality co-located to one ACC. This site takes over full NMS functionality if the primary NMC fails to operate. The standby NMC provides a northbound interface (NBI).

  Both primary and standby NMC provide a northbound interface that delivers aggregated information to the National Umbrella Management System (CGTEC) which is overlooking all ATM operation (not only the network).

- RMC (ACC): The Regional Management Center (RMC) is responsible for the planning and monitoring of the ACC sectors and the attached Radio Sites.

- APP: Mainly responsible for local management. Coordinated by the ACCs.

- RS: Radio Sites (RS) are on the lowest level of Management. They are unmanned and are managed by ACCs and APPs. Local Monitoring Options should be available if an engineer goes on Site.

2.3 The Data Collector queries or collects the information from all local elements. It can filter the content and performs data optimization before being forwarded to the Network Management Database.

2.4 Every time data crosses a data collector, the information is filtered and only the necessary content is forwarded. With this strategy, the amount of used bandwidth, but also the space needed on disk is kept at a reasonable amount. Aggregation is also defined by the reduction of information content if it is older than a predefined time (e.g.: older than 3 months).

2.5 Data Collectors mitigate the problem of preventing data loss during network interruption and/or insufficient available bandwidth. The data will be cached until they can be transmitted once the connection is re-established again.

2.6 The information needs to be transferred from the lowest element in the hierarchy up the chain to the top. The picture below shows the flow of the collected data. Monitoring can easily create a bandwidth shortage and puts unnecessary load on network devices when not properly designed. This is an important part of the solution to use data collectors close to the data source for efficient bandwidth usage.

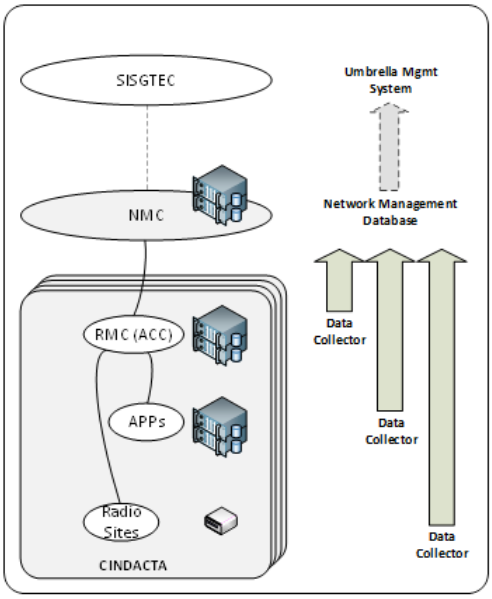

Figure 1 – Collected data flow

2.7 Only the National Level (primary and standby NMC) has a dedicated instance of the network management database server. This allows business continuity for the management services, even in case that the primary NMC is affected by disasters. The management server and its database are provided in a full redundant fashion, circumventing any single point of failure.

2.8 Data Collectors are deployed fully distributed as close to the monitored equipment as possible. In case of any interruption of communication between the Data Collector and the management server, the Data Collector does cache all measurements and events. Therefore, any important events or measured values can be accessed once the communication is resumed.

2.9 The Data Collectors come with a local web interface that allows local operators to resume monitoring function with a GUI similar to the one of the NMC but limited to the local scope. That allows gracefully degraded operation of monitoring in the case of a isolation from the NMCs in Rio de Janeiro.

2.10 These are the main benefits of this architecture:

- Each region can act independent from the other region. Outages in one region do not affect operation of other regions.
- The solution is bandwidth optimized due to the concept of data compression in the Data Collectors.
- Network outages does not cause loss of data – Important for problem analyses afterwards (especially during brown-outs).

2.11 Fault monitoring is one of the core capabilities that offer real time information about status changes of monitored elements that are part of the network infrastructure. The network infrastructure is learned by using auto-discovery or by “seed-file” based discovery. As a result the infrastructure is modelled at physical, logical and application layer. A wide range of standard and proprietary devices like routers, switches, firewalls, servers and other IT- and Telecommunication systems in its standard library are supported.

2.12 The discovery and device polling processes can be easily customized using XML templates. Devices can be also added and removed manually, if necessary.

2.13 Advanced multi-method, multi-thread discovery mechanisms ensure to keep the inventory database up-to-date with the necessary information for all monitored devices and services in the network.

2.14 It also detects the network elements and determines the physical and logical topology automatically. It uses SNMP to collect information from the devices on the network, allowing all devices that supports SNMP to be monitored by the system.

2.15 The solution makes use of a multi-user graphical user interface that allows user-defined levels of visualization and action over the alarms (i.e.: acknowledgement and clearance). In an example, the administrator can quickly navigate by selecting devices in the inventory browser, in the geographical topology and service status maps. Users can also be deployed by region, having their visualization and access of devices limited to their specific localization only. All data activity is logged, and these logs can be stored and furtherly processed externally.

2.16 The workflow management tool is used to guide through an approval process.

2.17 For safety reasons the Configuration Management tool and the Element Management tools are not prohibiting any changes to be made. The workflow management does not execute any configuration changes by itself on a technical level. Instead all decisions, which changes shall be made have to be decided by humans only. There are no technical automated decisions made to the system, triggered by the workflow management system.

2.18 In this way actions can be executed quickly if required operationally, even if the pre-configured workflow is not prepared for the actual situation.

2.19 The workflows are only used to guide all the stakeholders thru a specific business process or use case. On the other hand, the workflow management tool holds a history of the steps that have been followed up by the individual stakeholders.

2.20 Different stakeholders may take part in the workflow management processes. The stakeholders of the various maintenance levels are shown as an example. The dotted line between the stakeholders indicates an aligned communication scheme which is supported by the workflow management system, so that direct communication between persons is not necessary anymore, but rather replaced by communication thru the workflow management tool. Therefore, the workflow management tool can guide

and trace all actions over time and monitor the progress for an individual workflow process. The picture below depicts the overall decision process helped by the Workflow Management Tool.

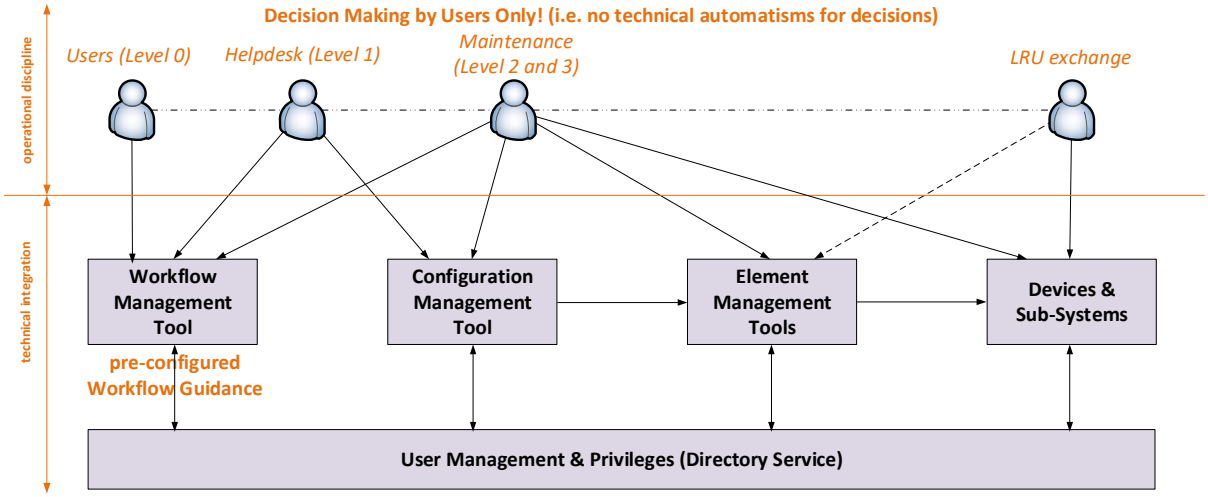

Figure 2 – Workflow management tool

2.21 A directory service is used for a unified user management, therefore any authorization needed by the tools (configuration management, monitoring, …) are controlled centrally. Therefore, any privileges needed for these tools are available independent of the location where these tools are accessed. A user with the respective privileges for viewing configuration settings can see these settings or differences thereof in the Configuration Management GUI.

2.22 The Configuration Management GUI gives visual access to event information when configuration changes were made. In these event messages it is possible to identify the user who has made the changes. From the time stamp in these messages and in the retrieved configuration changes, one can also see the difference of the configuration settings. These differences can be highlighted for better visibility.

3. Suggested actions

3.1 The meeting is invited to:

a) Note the information contained in this information paper; and

b) discuss any relevant matters as appropriate.
