siriOSS® iNMs

Network and Fault Management System
Ensuring smooth operations and optimizing asset performance

Smooth and reliable performance is important in industries and telecommunications. If delivery contracts are not fulfilled, contract penalties will be severe. In case of accidents the human, economic and ecological repercussions might even be catastrophic.

In short: Failure is not an option and a state-of-the-art network and fault management solution is needed to ensure smooth operations.

Atos siriOSS iNMs is the computerized solution for industry facilities that complements the various SCADA (Supervisory Control and Data Acquisition) systems by monitoring your assets and services in order to keep them operating safely and economically throughout their entire lifecycle.

iNMs manages and maintains all kinds of telecom- and IT-related assets, like servers, switches, base stations, transceivers, etc., including the required cabling. Within seconds iNMs delivers a transparent end-to-end view of the entire IT and telecommunications infrastructure and optimizes asset performance. Of course it fully complies with local regulations.

siriOSS iNMs detects network faults long before your staff will notice any deviations in their service. Whenever any divergence occurs, it correlates and filters the alarms sent out by the affected network elements and performs a root cause analysis. It then automatically issues alarms and trouble tickets or triggers further actions, giving you the chance to immediately initiate countermeasures.

Additionally, siriOSS iNMs provides features to increase the performance and service quality of your solutions and prevent faults.

siriOSS iNMs is an umbrella management solution (multi-vendor, multi-technology and multi-domain), joining and correlating information from all kinds of electronic sources, including complementing SCADA systems. It is highly scalable and can monitor thousands of elements simultaneously.

siriOSS® iNMs (integrated Network Management services)

- Alarm reduction by 97%
- 95% of the remaining alarms are managed automatically
- Overall workload of operators reduced by 20%
- Integration of complete networks within weeks.

Typical results achieved in international projects

Trusted partner for your **Digital Journey**

Atos

Network Repository

The repository of iNMs stores all the network information and provides a uniform view of the heterogeneous network with different visualization options, like alarm lists, topology-view, GIS-view or floor plans. Network information is entered consistently and easily by Autodiscovery (topology and network element information is automatically retrieved from the network), Manual Configuration or Batch import/export (in CSV format).

Network Monitoring

iNMs receives alarms via its various network interfaces (e.g. SNMP, in the form of traps) from the network. In order to reduce the alarms that occur in a network, different rules for correlation and alarm filtering can be defined.

iNMs provides alarm tables as well as graphical representations for each of the monitored components. Alarms are color-coded in line with their severity. Alarms for network components are indicated on the GUI in the color representing the highest severity. In addition, iNMs saves alarm log information.

For easier handling of complex network structures the network can be divided into management areas by creating domains. Domains can contain network components and other domains, and can overlap as desired.

Performance Monitoring

In addition to alarms and other events, iNMs also processes performance data. Typical KPIs include processor load, disk space usage or IP connection performance (delay, jitter, packet loss). iNMs can create alarms when defined thresholds are reached.

Service Management

A service is a combination of functionalities distributed across the network and its network elements which fulfills a specific purpose from user perspective. A typical example of an end-to-end service is a customer's communication link. iNMs is capable of defining, monitoring and graphically representing end-to-end services and their statuses.

Root Cause Analysis

To prevent faults the system analyzes trends and proactively increases the service quality of the network and its connected physical and virtual applications. If a problem occurs, it detects faults through filtering, correlation and root cause analysis. Reactions are automatically initiated and trouble tickets generated.

Reactions

Typical reactions include:

- the output of an acoustic signal,
- the transmission of error messages via e-mail,
- the forwarding of alarms (original ones as well as new ones created by iNMs) to other systems, e.g. trouble ticketing, and/or
- the automatic execution of programs for error analysis or error correction.

Reactions can be initiated on a context-sensitive basis as well as on a time-constraints basis (e.g. "nights only").

High usability

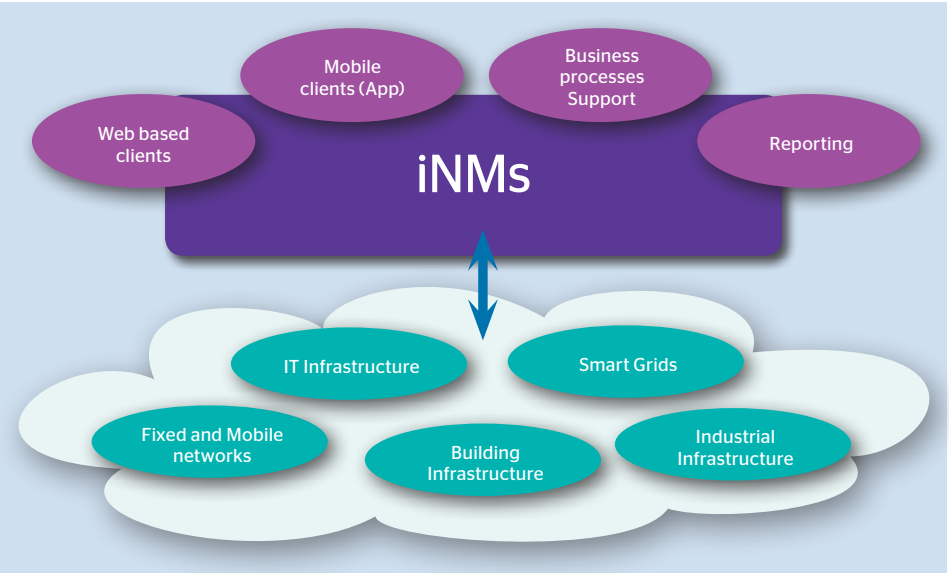
All relevant information is displayed in an easy-to-understand format on flexible and customizable dashboards, which feature several different visualization options, such as traffic lights and data sheets. Operators can select individualized monitoring profiles and adjust them via drag and drop to fit their requirements and expertise level and ensure smooth performance.

Reporting

iNMs evaluates and graphically represents alarm data as tables or HTML files, using bar charts or pie charts.

Full CMMS Support

CMMS (Computerized Maintenance Management System) focuses on a consolidated maintenance database which contains all the necessary information about maintenance activities. siriOSS iNMs can be extended by other products of siriOSS suite to cover CMMS functionality and can be easily integrated with other vendors' products for any other modular CMMS solution.



For more information: **+40 268 409 400 / info-cc@atos.net / atos.net/convergence-creators**

CT_180307_AS_siriOSS-iNMs