

Sentinel



Description

GE's **Sentinel** is a management solution for supervising complex private networks, providing a single platform that aggregates, correlates and visualizes telecom data from multiple network layers and technologies into user-oriented views. This solution drives operational decisions to maintain service availability, assure prompt service restoration, proactively notify users of potential service impacts, meet network KPIs, and continuously monitor the quality of delivered services. This in turn helps assure the fulfilment of quality obligations and contractual SLAs.

Key Benefits

- **Enhanced Operator Awareness** for fast fault detection and localization, proactive management (detect anomalies before users), reduced downtime, efficient usage of work force, and reduction of maintenance costs.
- **Enhanced User Awareness** for the proper operation of mission-critical applications, prompt information on services impacted by network anomalies, and assurance that service requirements are constantly fulfilled.
- **Single source for network information.** Sentinel inventory provides a coherent and unique source of information common to functions such as network operation, maintenance, transformation projects, planning, etc., facilitating exchanges between network management actors and stakeholders.

Core Capabilities

- Integrated management of complex multi-vendor networks
- Prompt fault localization
- End-to-end availability monitoring and measurement
- Rapid deployment irrespective of legacy technologies

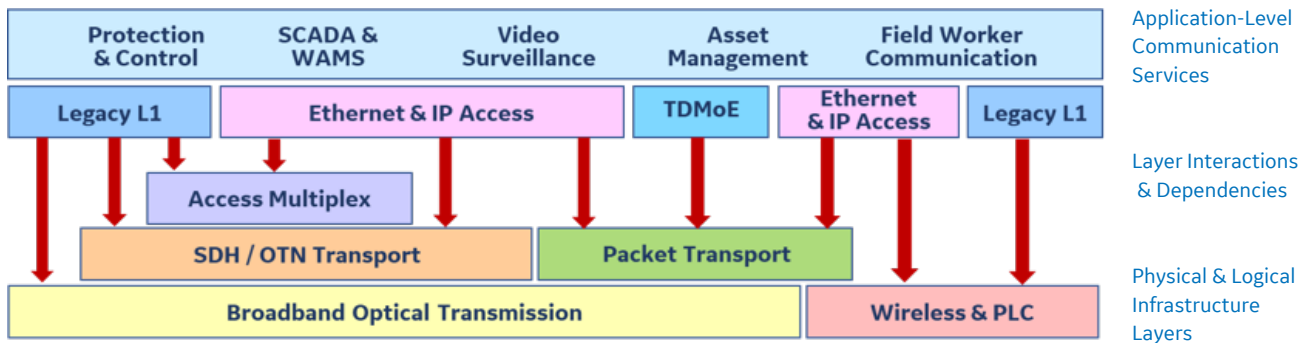
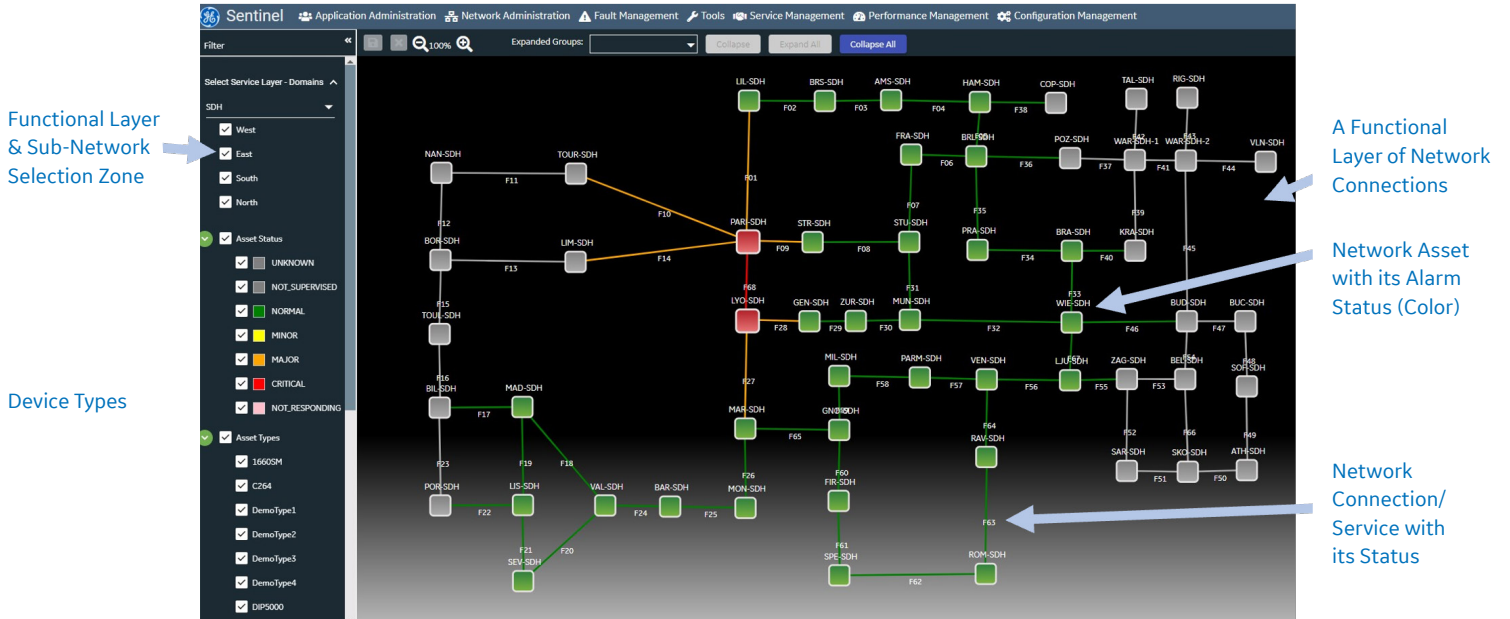
Key Features

- Functions, scale, and cost optimized for grid operational communication networks
- Fault, performance, and incident management in a single integrated platform
- Service user dashboards, impact notifications, and service statistics

Optimized Outcomes

- Enhanced operator awareness & proactive management
- Formal and documented communication service delivery process & user-provider relations
- Structured framework for network information



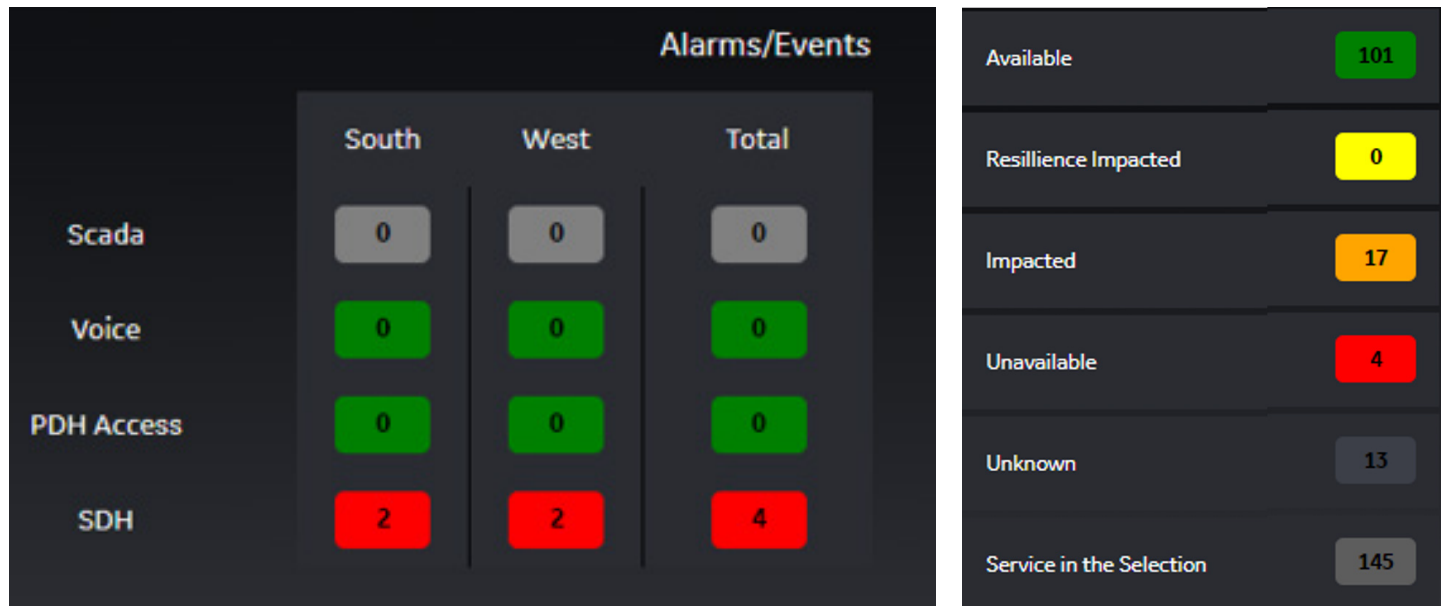


Modeling and visualization of network overlays frequently encountered in operational communication networks. These networks are developed and renewed over many years, hence integrating new and legacy technologies and multiple technology overlays. The top figure presents the physical or logical connectivity at one layer of the network.

Features

Sentinel combines real-time supervision and network/device data inventory functions to deliver situational awareness on telecom network and communication services and to enable interactions between network stakeholders.

- **Multi-vendor & multi-technology.** An operational network is built over years and integrates generations of legacy technologies and devices from multiple vendors. Sentinel covers the whole network with varying degrees of visibility, according to available information.
- **Easy-to-deploy, operate, and maintain.** Provides a powerful solution for monitoring, supervising, and reporting on devices and services at grid scale. Focused on features relevant for the operational network, reducing cost, complexity, and training.
- **Fully under utility control.** Resides entirely inside the power utility's operational security perimeter.
- **Service-based principles.** Elaborates a full picture of any service plane into a display irrespective of technologies employed for its delivery, hence facilitating supervision (SCADA over circuits and over IP).
- **“Avalanche of Alarms” resolution.** Major failures such as cable disruptions impact a large number of overlay connections and generate many alarms. Sentinel allows rapid identification of the root cause to initiate restoration, as well as fast detection of all service impacts to notify impacted users.
- **Interaction platform for actors and processes.** Comprises incident assignment and handling, fault and service notifications, intervention reporting, and service user/provider relations.
- **Standard interface points.** Requires very little from supervised devices and connected applications (SNMP, dry contacts, web-service, customer-defined executable scripts), enabling legacy integration



The Fault Dashboard produces a synthetic view of active alarms across the selected layers and zones of the network. A companion table provides the distribution of connections/services in the selection according to their status (available, unavailable, etc.). This provides a high-level awareness of the network's operational health.

Key Benefits

Enhanced Operator Awareness

- Produce a unified view of network devices, services, alarms, and operations
- Enable operations team to monitor and maintain a multi-layer network with inter-layer interactions
- Reduce the need for specialist intervention time by empowering network operators to perform fault detection and localization using Sentinel
- Associate fault data with network configuration data for problem solving
- Simplified detection & localization of network faults through powerful root cause analysis
- Determine service impacts of a network fault
- Monitor network performance at identified points to constitute a network behavior signature
- Maintain a log of all operator-initiated actions

Proactive Management

- Reduce service outage perception by detecting faults before service users do
- Fast service impact analysis and selective user notification of service loss due to network faults
- Notify users when disrupted services are back to normal
- Detect catastrophic failures to adjust from normal to disaster mode maintenance process

Enhanced User Awareness

- User-focused service management, service dashboards showing the state of wide area connections
- User notification of service impacts due to network faults
- User SLA monitoring for different services and proof of fulfilment of service quality commitments
- Statistical service outage metrics and monthly service reports

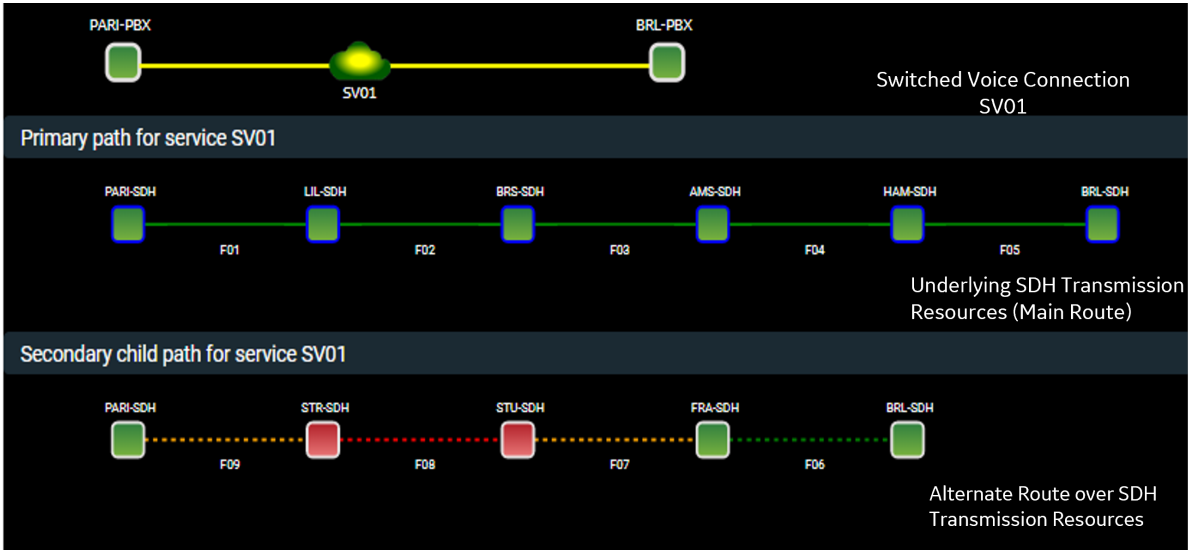
Incident Resolution & Service Restoration

- Prompt, structured handling of network faults
- Reduce service restoration times
- Assign and resolve incidents through networking of all concerned actors
- Orchestrate network and service restoration (incident management)
- Assign the right actors & provide all necessary information
- Facilitate remote access to tools
- Enable interactions for network actors through a unique framework
- Prompt root cause and service impact analysis
- Keep track of open incidents and generate statistics on incident resolution

Service & Network Off-line Data – Network Inventory

- Provide a unified source of device, network, and service information for all network management actors
- Device data and configurations, physical & logical network maps, underlying infrastructure Path Finder functionality, service data & user contacts, inter-layer network dependencies
- Contingency analysis and “what if” scenarios to simulate impact of network faults and scheduled outages
- Generate coherent and relevant data for different stakeholders (user, service manager, network supervisor, intervention staff, etc.), combining real-time and inventory data

Sentinel Data Exploration



Root Cause Analysis & Path Track identify underlying infrastructure and their fault propagation

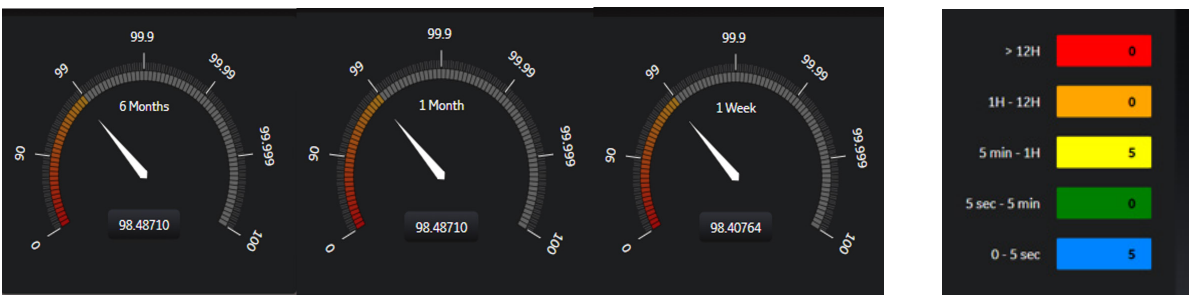
Analyzed Resource

Type	Service Layer	Service Name	Main Path	Alternative Path	Input Asset	Output Asset
Analyzed Service	SDH	F68			PARI-SDH	LYO-SDH
Impacted Service	WAN Tunnels	DC05	Y	N	MAD-SW	PARI-SW
Impacted Service	PDH	MC01	Y	N	PARI-PDH	WIE-PDH
Impacted Service	PDH	MC04	Y	N	PARI-PDH	LYO-PDH
Impacted Service	Scada	SC05	Y	N	MAD-CC	PARI-CC
Impacted Service	Voice	SV08	Y	N	LYO-PBX	PARI-PBX
Impacted Service	Voice	SV09	Y	N	PARI-PBX	MAD-PBX
Impacted Service	WAN Tunnels	DC06	N	Y	MAR-SW	MAD-SW
Impacted Service	PDH	MC07	N	Y	MAD-PDH	PARI-PDH
Impacted Service	Scada	SC02	N	Y	VEN-CC	PARI-CC
Impacted Service	Voice	SV13	N	Y	MAR-PBX	MAD-PBX

Overlay services using the resource

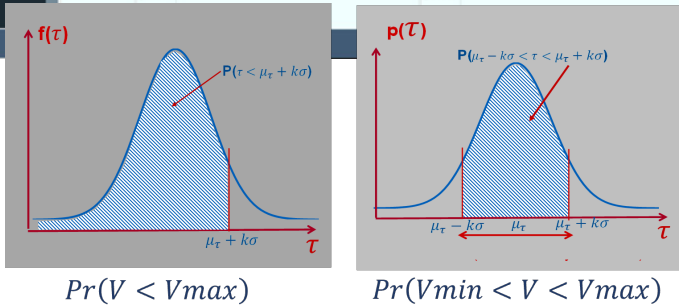
Service Impact Analysis identifies services impacted by a faulty resource in the underlying infrastructure

Service Availability and Outage Distribution



Availability for selected services: Over last week, last month, last 6 months, and Monthly Service Outage occurrences with durations of <5sec, 5 sec-5 min, 5 min-1H, 1H- 12H, and >12H

Sentinel Performance Value Collection, Data Storage, and Statistical Estimation



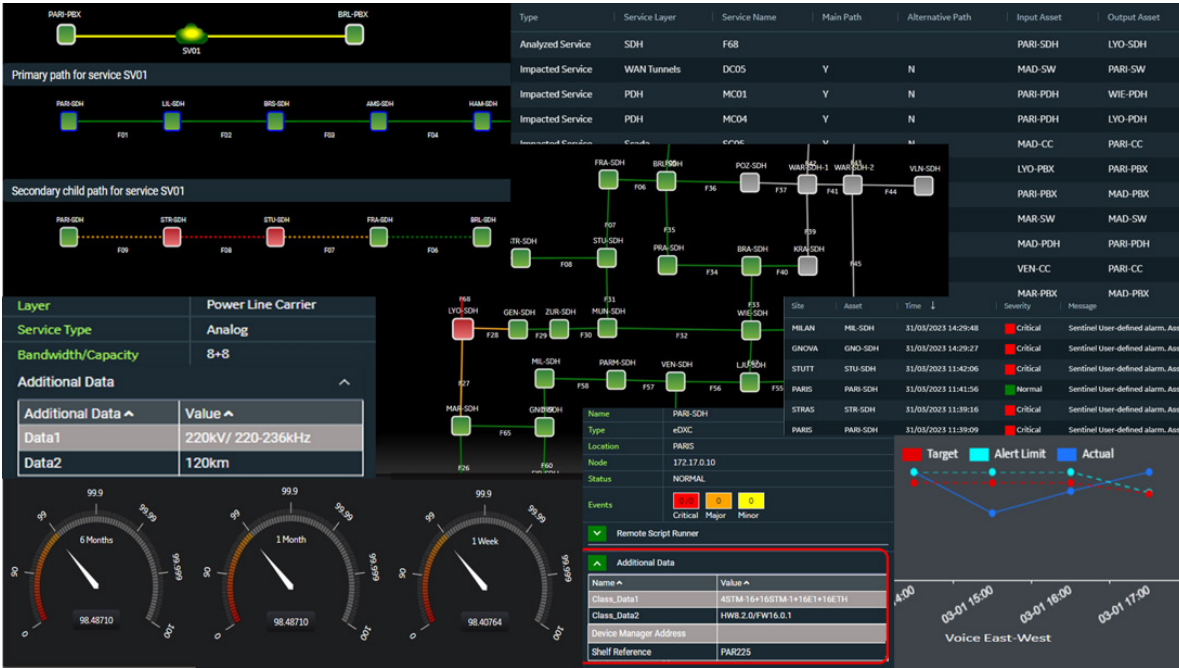
One-sided and two-sided Gaussian-model probability estimations - limiting values for 95%; 99% and 99.9% probabilities

Name	PARI-SDH
Type	eDXC
Location	PARIS
Node	172.17.0.10
Status	NORMAL
Events	0/0 0 0 Critical Major Minor
Additional Data	
Name ^	Value ^
Class_Data1	4STM-16+16STM-1+16E1+16ETH
Class_Data2	HW8.2.0/FW16.0.1
Device Manager Address	
Shelf Reference	PAR225

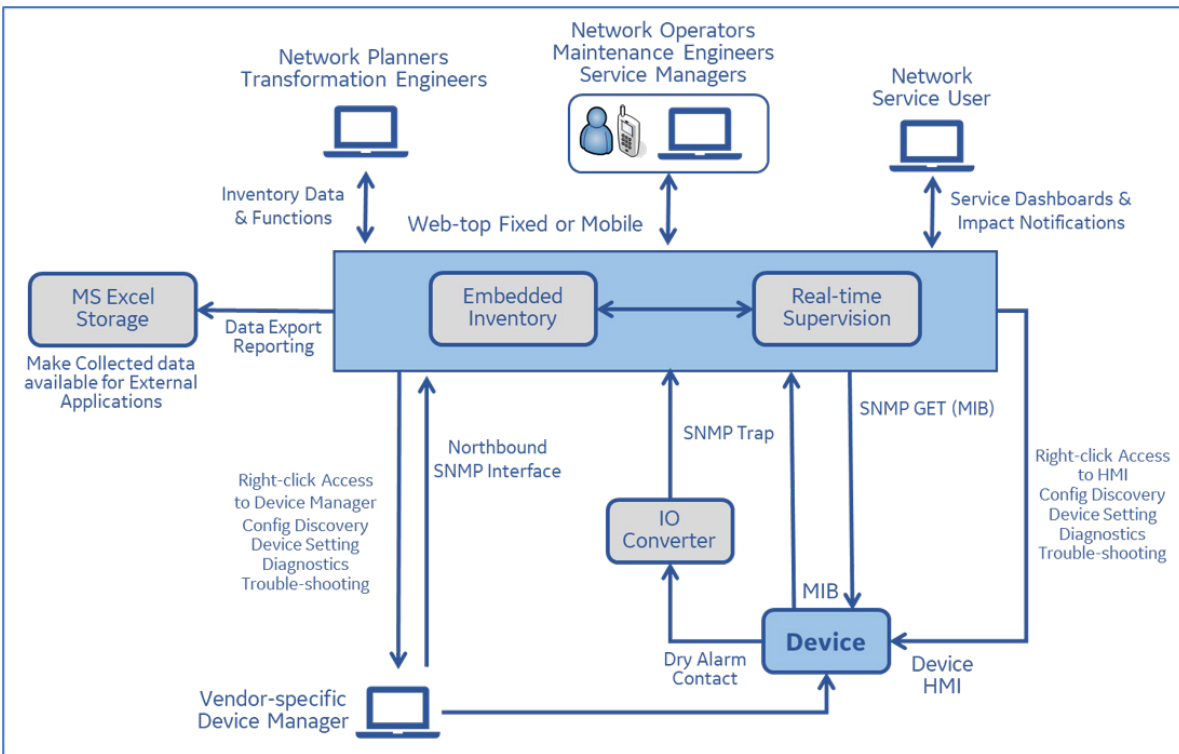
SERVICE	
Name	PL01
Input	PLC 01
Output	PLC 02
Layer	Power Line Carrier
Service Type	Analog
Bandwidth/Capacity	8+8
Additional Data	
Additional Data ^	Value ^
Data1	220kV/ 220-236kHz
Data2	120km

Examples of Asset and Service Inventory Data fields. Asset data for an SDH multiplexer provides a brief description of device configuration, hardware version and firmware release, dedicated device manager address and the cubicle in which the device is installed. The service data for a PLC link provides service type, frequency band and bandwidth usage, line voltage and link distance.

MANAGEMENT FUNCTIONS	SENTINEL 4.0
Fault Management	Technology- and vendor-agnostic multi-layer displays Automatic node discovery with manual assignment Alarm monitoring (event list, graphical supervision) and filtering (time, functional layer, sub-network) Fault detection, localization, and root cause analysis Generic and simple web-based UI and template-based operation Rule-based notification (alarm/event, time of day, service statistics) Operator-initiated change of state
Incident Management	Incident ticketing, task assignment, escalation and intervention reporting Interaction of O&M actors via incident handling functions and free-format whiteboard messaging service Incident resolution statistics & dashboard Asset & service tagging and work order
Service Management	Generate service availability and outage statistics Monitor service level agreements (SLA) Service-oriented selective user dashboards MS Excel report generation (performance, alarms, incidents)
Performance Management	Monitor-point (MP) setting and scheduling MIB-stored performance value retrieval and monitoring Monitored value storage and statistical processing Gaussian model min/max values estimation for 95-99.9% probability
Inventory Management & Configuration	Device & network inventory storing basic configuration data Asset & service data available on a click Physical inventory data down to physical interface and cubicles Logical inventory covering peer-to-peer connections, service dependencies, bandwidth usage, device logical ports and VLANs. Additional data fields set according to user-specific requirements Site geographic coordinates & map display Manual data population or MS Excel/CSV import files Inventory data export as Excel file Multi-criteria inventory search engine exploring for assets and services Intervention & notification contact coordinates (user, expert, field staff, etc.) Show underlying infrastructure for any service (Path Track) Resource bandwidth/capacity usage estimation (bandwidth management) 1-click access to proprietary element managers & HMIs
Security Management	Role Based Access Control (RBAC) Password protection for server access Security certificates for unambiguous server identification Encrypted web-service & client-to-server links Encrypted device-to server links (devices supporting SNMPv3) Authentication through RADIUS server Sentinel Operator & System Log Management
Mobile Worker Terminals	Web-based user interface allowing any terminal with a web browser (PC, tablet, smartphone) Dashboards, event list, notifications, incident assignment and reporting



Sentinel provides numerous analytic displays accessible according to installed capability packages and defined roles and profiles of the system user, providing clear insight into the network's operation.



Data sources and exchanges in GE Sentinel management paradigm

ADDITIONAL TECHNICAL DATA

N-tiers application based on a service-oriented architecture model

Sentinel Clients require only a web browser. No limit on number of simultaneously open clients

RedHat Linux Server, redundancy (option) through asynchronous data replication

PostgreSQL database

Number of supervised nodes determined by license size (from <100 to >2000)

Can be re-adjusted by license upgrade

Embedded MIB Files - GE communication portfolio device MIBs by default

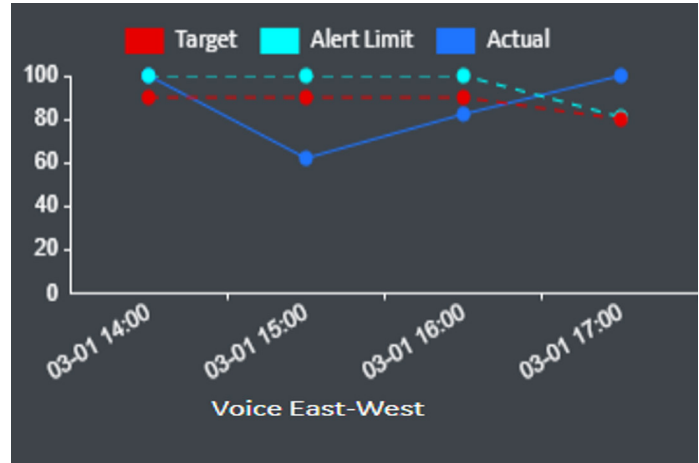
Can load other SNMP device MIB files

Sub-networks & functional layers - Unlimited functional layers partitioned into multiple regional sub-networks.

Can regroup multiple nodes into a grouped node.

Management functions are grouped into functional capability packages and may be added through license upgrades:

- Basic By-Default Functions – Fault Management, Network Inventory
- Situational Alert – Event Notification by Mail/SMS, Script Execution, Northbound Interface (NBI)
- Data Explore – Root Cause Analysis, Service Impact Analysis, Bandwidth Management, Path Track
- Incident & Work Order – Incident Handling, Incident Resolution Dashboard, Tagging & Work-flow
- Performance Monitoring – Performance Monitor Setting & Scheduling, MIB Value Retrieval, Statistical Estimation, Performance Dashboard, MS Excel Value Export, MIB/SLA Monitoring
- Network Fault Simulator – Contingency Analysis (“What if” scenarios)



Monitoring SLAs with Actual, Target and Alert limit values

For more information please contact
GE Power
Grid Solutions

Worldwide Contact Center

Web: www.GEGridSolutions.com/contact
Phone: +44 (0) 1785 250 070

GEGridSolutions.com

IEEE is a registered trademark of the Institute of Electrical Electronics Engineers, Inc.

GE and the GE monogram are trademarks of GE.

GE reserves the right to make changes to specifications of products described at any time without notice and without obligation to notify any person of such changes.

© Copyright 2023, GE Company. All rights reserved.

