Digital Energy

Sentinel

Monitoring and control of multi-layer operational networks and services

TRANSFORMING COMMUNICATION INFRASTRUCTURE DATA INTO NETWORK AND SERVICE INTELLIGENCE

The challenge for Power Utilities in implementing their Operational Communication Network is how to manage an evolving, multi-technology, multi-vendor telecom infrastructure to deliver services with a guaranteed level of quality for multiple groups of users with different service requirements.

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

DIFFERENTIATING 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
- Documented & formal communication service delivery
- Structured framework for network information
- Comprehensive cyber security solutions

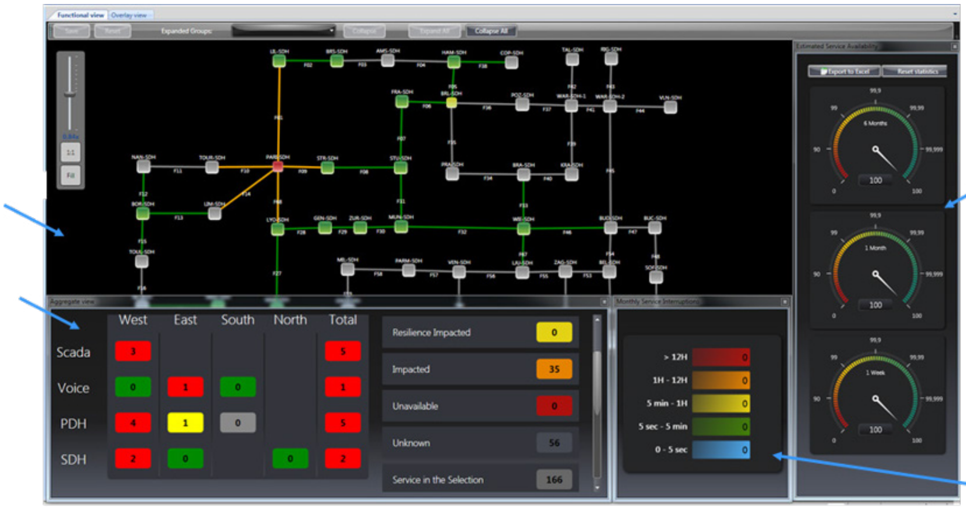
OVERVIEW

GE's Sentinel delivers a management solution for supervising multi-technology complex networks. Providing a platform that aggregates, correlates and visualizes telecom data from multiple network layers and technologies into user-oriented views, driving operational decisions to restore services, notify users of potential service impacts, and meet KPIs and performance metrics.

The result? Greater efficiency and productivity. Assure mission-critical applications through enhanced monitoring of communication services and infrastructures. And reduced down-time and maintenance costs.

Sentinel

Monitoring and control of multi-layer operational networks and services



	West	East	South	North	Total
Scada	3				5
Voice	0	1	0		1
PDH	4	1	0		5
SDH	2	0		0	2

Resilience Impacted	0
Impacted	35
Unavailable	0
Unknown	56
Service in the Selection	166

> 12H	0
1H - 12H	0
5 min - 1H	0
5 sec - 5 min	0
0 - 5 sec	0

Network Layer Status

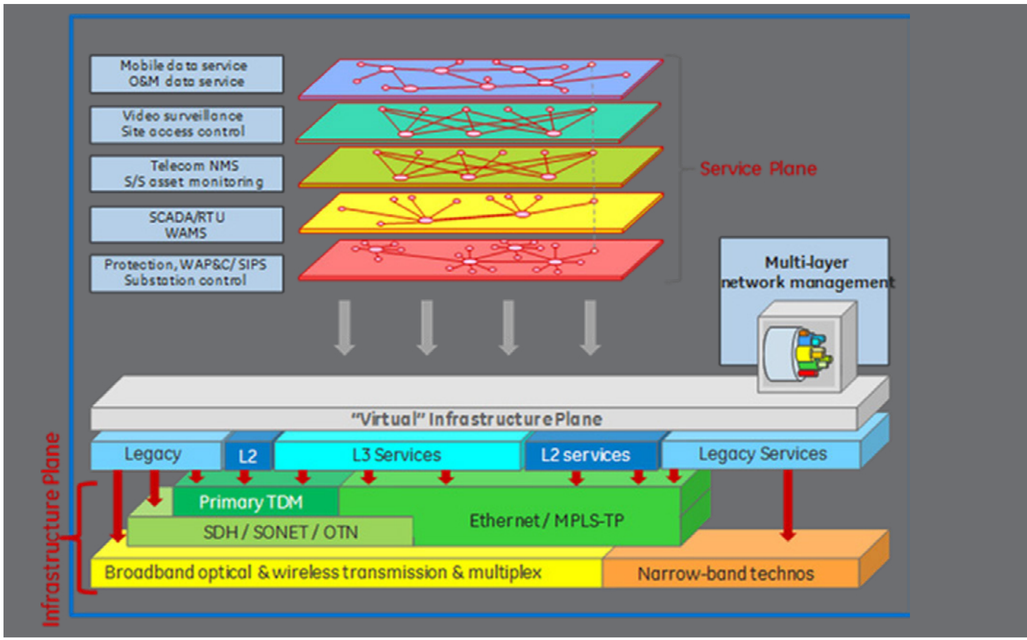
Aggregate Alarms & Service Status

Network Layer Service Availability

Network Layer Service Outage Distribution

Sentinel is a vendor-agnostic management platform designed to fulfill the requirements of power utilities' operational communications.

- **Multi-vendor and multi-technology** – Allows flexible construction of the network with best suited building blocks without committing for the future to any specific single vendor.
- **Easy to deploy, operate, and maintain** – Provides a powerful solution for monitoring, supervising and reporting on devices and services at grid scale restraining to features which are relevant for the operational network, hence reducing cost, complexity, and learning effort.
- **Fully under Utility control –** Resides entirely inside the power utility's security perimeter.
- **Service-based principles** – Associates multiple technologies into the delivery of a single operational service plane (TDM and IP SCADA), facilitating supervision.
- **Root Cause Analysis, Service Impact Detection** Assists the operator in determining alarm avalanche origin.
- **Interaction platform for actors and processes** Comprises incident management and trouble ticketing facilities, mailing facilities for service- related communications, and reporting facilities for maintenance management and user/customer contractual relations.
- **Standard interface points** – SNMP, web-service, customer-defined executable scripts



Fault & Incident Management

Technology- and Vendor-agnostic End-to-end and multi-layer vision

Generic and simple UI (No specific skills)

Enable interaction of O&M actors (including remote clients, field tablets and smartphones)

Assist in network fault root cause analysis

Rule-based notification (event, time, statistics)

Performance Management

Generate service availability/outage statistics

Monitor service level agreements (SLA)

Monitor MIB-stored performance data

Service-oriented User Dashboards

Configuration Management

Store basic Network configuration data

Maintain Asset information

Manual data population or CSV import files

Site Geographic location coordinates

Contact Coordinates for incidents, interventions and notifications (user, expert, field staff, ...)

Unified access to vendor tools and platforms

Security Management

Role-based access control (RBAC)

Password protection for server access

Security certificates for unambiguous server identification

SSH tunnel between client and server

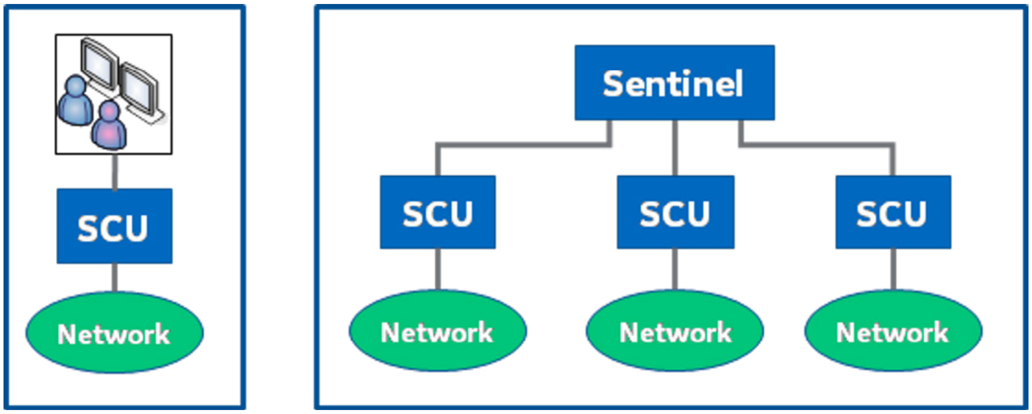
Operator log management

Authentication through RADIUS server

Secure access for third party systems

Sentinel Control Unit (SCU)

Managing faults from a relatively small cluster of equipment, typically communication devices in a few substations or a single type of equipment, requires a compact and factory-prepared solution. The Sentinel Control Unit (SCU) provides a hardware-integrated ready-to-use management platform for simpler/ smaller networks (~ 60 nodes). This allows to deploy a small supervision system even faster.

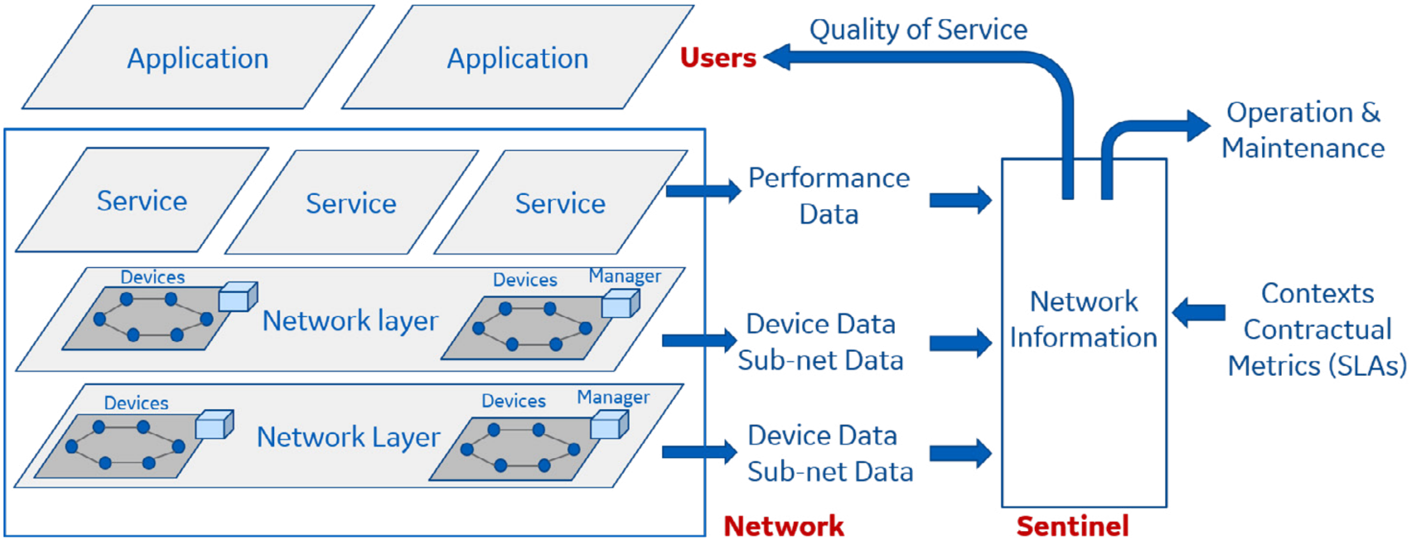


The substation-class hardware allows the platform to be installed in a harsh industrial environment such as an electrical power substation for a cluster's SNMP management removing the need for an expensive industrial PC. It can be mounted into a DIN-rail cabinet next to communication or protection signaling devices and supplied from a substation 48Vdc battery and charger source.

The SCU may also be used as a secondary-level platform in a hierarchical architecture for large networks. In this way, a north-bound SNMP interface at the SCU can be configured so that alarms on the SCU generate a collective event at the higher level platform. The operator can then connect to the SCU (as a client) to get more detailed indication on the alarm cause.

Connection to remote web-based client is protected with all relevant security embedded into the system (encryption, authentication server, etc.).

Sentinel Management Framework Operational Principles



Sentinel collects alarms and events as well as service performance data from devices and dedicated managers, associates contextual network and quality constraint information to the real-time collected data, and consequently generates operation and maintenance information for the communication service provider and quality of service information for the service users.

Sentinel

Monitoring and control of multi-layer operational networks and services

Features Comparison

As indicated previously Sentinel Control Unit (SCU) serves a different role from the "regular" RedHat Linux server based Sentinel. Their features and functions are consequently not identical as highlighted in the table below. The SCU is focused on the monitoring of a cluster of devices in one or multiple substations. It is

designed for installation in severe environment and rack mounting as opposed to a more Network Operation Center environment and network-wide capacity and capability of the server-based system.

Feature	Sentinel Conventional Server 3.6	Sentinel Control Unit (SCU)
Number of network nodes (max)	Up to 2500 nodes (graphical)	60 nodes (expandable to 100 in specific cases)
Number of Clients	Up to 20	2
Server Redundancy	Yes	Not at present
Fault Management	Alarm Monitoring (Graphical & Event List), Filtering, De-duplication, Acknowledge, Rule-based Notification, Operator-based Change of State	Alarm Monitoring (Graphical & Event List), Filtering, De-duplication, Acknowledge, Rule-based Notification, Operator-based Change of State
Incident Management	Trouble ticketing, Task Assignment, Escalation, Intervention Reporting, Asset & Service Tagging, Resolution Statistics	Trouble ticketing, Asset & Service Tagging, Resolution Statistics
Service Management	Service Availability Statistics and SLA Monitoring	Service Availability Statistics and SLA Monitoring
Security Management	Role-based Access Control (RBAC), Encrypted Web-service and Client to Server links, Encrypted device to server links (for SNMPv3 only), Client Authentication (RADIUS), User Log Management	1 client with full rights and encrypted link to SCU Encrypted Web-service and Client to Server links, Encrypted device to server links (for SNMPv3 only), User Log Management
Performance Management	MIB Monitoring on demand	MIB Monitoring on demand
Configuration Management	Asset & Service data available on right- click Shows underlying assets and links for any service Connectable to a Network Inventory Connects to proprietary Element Managers and HMIs	Asset & Service data available on right- click Shows underlying assets and links for any service Connects GE portfolio Managers and HMIs
Embedded Management Files	Incorporates GE portfolio device MIBs Can load other SNMP device MIBs	Incorporates GE portfolio device MIBs (For other SNMP device MIBs consult GE Ucom)
Sub-networks & Functional Layers	Up to 10 functional layers each can be partitioned independently into multiple sub-networks. Can also regroup multiple nodes into a Super-node.	Up to 3 functional layers Can regroup nodes on each layer into Super-nodes
Mobile worker terminals	Mobile (Android) Dashboards, Event List, Incident assignment and reporting	Mobile (Android) Dashboards, Event List, Incident assignment and reporting

Digital Energy

Sentinel

Monitoring and control of multi-layer operational networks and services

Technical Data

ARCHITECTURE

N-tiers application based on a service-oriented architecture model
OS: RedHat Linux (server) - Windows 10 (Client)
Microsoft.Net (Client) - Java (server) - PostgreSQL (database)

AVAILABLITY

Server redundancy through asynchronous data replication

DIMENSIONING DATA

More than 1500 assets and 10 layers according to licence. 60 assets and 3 layers for SCU
Can be organized into sub-networks and grouped nodes and services

NUMBER OF CLIENTS

Up to 20 through separate licences

ALARM MANAGEMENT

Alarm reduction (de-duplication) - Multiple alarm indications provided by the same event and element are removed (grouped) to avoid flooding the operator
Alarm priority and acknowledge
Alarm refinement - Alarm labels may be translated into explicit and vendor independant language
Operator-initiated change of state and status consistency check

INCIDENT MANAGEMENT

Task assignment and tagging (assets and services)
Incident resolution statistics

SERVICE MANAGEMENT

Service availability statistics and user dashboards
MIB element monitoring for all SNMP devices

PROBLEM MANAGEMENT

Root cause analysis - Dispatch of alarms and events across multiple layers of infrastructure and service in order to visualize the root cause anomalies

EVENT REPORTING AND NOTIFICATION

Service level monitoring with temporal analysis
Generates triggers on event conditions (asset and service status, service statistics, time of day) used for different actions (audible alert, SMS, email, script execute)
Pre-determined report generation (performance, alarms, incidents)

SECURITY AND AUTHENTICATION

Password protected, role-based authorization (RBAC), encrypted web services
Client authorization using RADIUS server
SSH communication tunnel between client and server, security certificates for unambiguous server identification

Contact Us
ge.com/digital/sales-contact-me