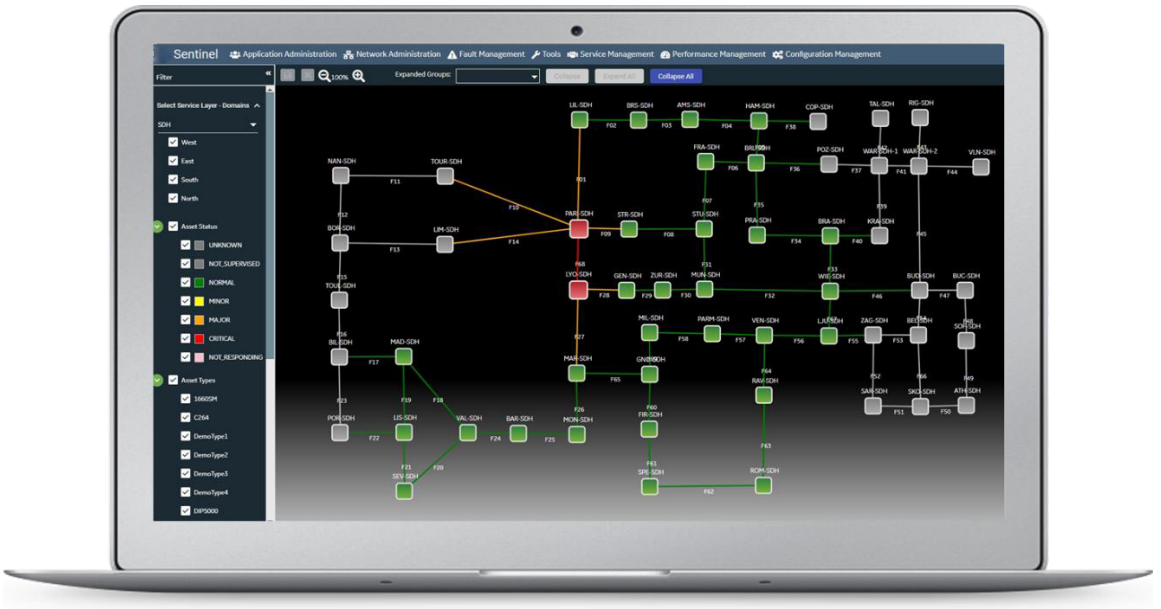
GE VERNOVA

A Guide for Network Planners

IMPLEMENTING A MODERN MANAGEMENT PROCESS FOR OPERATIONAL COMMUNICATION NETWORKS USING GE VERNOVA SENTINEL

Whitepaper



Grid Solutions

WARNING

This document describes GE Vernova Sentinel platform at a given instant of time. As such it is not contractual or binding in any manner. It should not be transmitted outside the company without prior permission.

1. INTRODUCTION

The digitalization of the electrical power system and the dispersed intelligence across the grid require extensive data exchange. The communication network in this context is increasingly an essential component of the new digital grid. It must provide reliable, secure, and prompt data exchange:

- from substation to substation between protection devices,
- between monitoring and control platforms and field-deployed "intelligent devices",
- between field intervention workforce at grid premises and support at technical offices.

Substantially increased number of connections, higher bandwidth, more flexibility, and faster service restoration are needed to enable the required services. An enhanced approach to communication service and infrastructure management is necessary to achieve these objectives in the operational network. This can be achieved by moving from isolated tools and default processes towards integrated platforms providing holistic situational awareness and enabling facilitated interaction of operational actors for prompt network adjustments.

Enhanced network management comprises prompt and easy supervision as well as a versatile information system to enable network planning, deployment, transformation, and operation. Network operators must rapidly relate captured network events and monitoring values with previously stored engineering data. Many diagnostics and problem resolution tasks require swiftly moving back and forth between the real-time supervision information and network/device engineering data.

GE Vernova Sentinel telecom network management solution exploits this association of real-time network state with network configurations and device information, hence allowing for a gradual implementation of an Operation Support framework integrating previously distinct information silos, network management tools and operational processes.

Deploying a full-scope telecom management system represents non-negligeable effort for the Power Utility. Some of the reasons that make it worthwhile are presented hereafter and summarized in figure 1 below.

a. **Enhanced Operator Awareness** – Operator's full awareness of the state of the network is essential for taking appropriate corrective action to restore service or to adjust network resource usage to service requirements and loads at any time. Network fault detection, localization, and root cause analysis, as well as the continuous monitoring of performance at some key points of the network constitute its main components. To be effective, fault and performance monitoring need to be performed through a unified and generic framework. Federating the siloed and proprietary telecom management systems under a unified platform brings the benefit of multi-layer network management by correlating events and states across different network constituents.

b. **Proactive Management** – Proactive management means being informed of anomalies before they are perceived by the applicative users. Prompt detection and localization of network anomalies (as described above), followed by fast identification of impacted services, allows the telecom network operator to notify users of service impacts, and to initiate the resolution of the incident by assigning it to the appropriate workforce as described in the next bullet point. Network anomalies analysis and service impact identification are recurrent, laborious, and time-consuming tasks which are largely simplified and accelerated through process automation implemented in Sentinel platform, hence enabling efficient usage of skills and expertise in the management organization in a context of growing operational network size and complexity.

c. **Fast Incident Resolution and Service Restore** – The resolution of network incidents can be accelerated through integration of incident management in the real-time supervision and network inventory framework. In this manner, the person or team assigned to resolve the incident has automatically access to all real-time supervision information and configuration data relating to the devices involved in the incident. An accelerated incident resolution process results in reduced service outage and more efficient usage of skills and expertise in the management organization.

d. **User Awareness & User-Provider Relationship** – Increasingly, operational Service Users expect the Service Provider to prove that contractual obligations defined through a Service Level Agreement (SLA) are being continuously met. The management framework is required to perform service impact analysis and notification, SLA monitoring functions, User service quality dashboards and monthly quality reporting.

e. **Data Repository for Network Transformation Planning** – Network planning, deployment, and transformation requires complete, coherent, and up-to-date information. A unique network inventory provides planners with a reference information base necessary for transforming and operating the network. In addition, planned devices, services and connections can be created in the base and activated when they are deployed. In this manner, the Network Inventory can serve as a change management and service provisioning workflow tool.

Enhanced Operator Awareness	**Unified generic view** of network devices and services together with their status. **Monitor SLAs** todetermine the fulfilment of contractual quality obligations for each group of users
Proactive Management	Prompt **Fault Detection & Localization** using multi-layer views and inter-layer interactions before perceived by service users. Determine **Root Cause and Service Impacts** of network faults reducing specialist staff mobilization on network incidents.
Fast Incident Resolution & Service Restore	**Generic skills** for the system operator with no vendor- or technology-specific knowledge. Efficient **incident management** by assigning resolution tasks and assuring interaction of relevant actors to reduce service restoration times. Keep track of **incident statistics.**
User Awareness & User/Provider Relationship	**User Dashboards** with Service Availability and monthly outage displays for each user group (SCADA, Protection & Control, Surveillance ...) **Notification of Service Impacts** of network faults to concerned users.
Network Planning Data Repository	Device and Service data are stored in the data repository and retrieved for problem solving or **transformation planning**. Service Impact simulation using **"What-if" Scenarios**

Figure 1 – Sentinel value proposition for Operational Communication Networks

This document presents the value proposition and some important use cases of Sentinel 4.0 context-aware management platform.

2. NETWORK MANAGEMENT FUNDAMENTALS: PROCESS, FUNCTIONS AND PLATFORMS

2.1. TELECOM MANAGEMENT PROCESS

Telecom management englobes all activities for implementing, transforming, operating, and maintaining communication services and the underlying network infrastructure. These processes are performed by people organized into specific roles. The management tools and platforms assist fulfilling these tasks and enable some degree of process automation. It is therefore important to bear in mind that network management is not just about software tools. It is primarily a process involving people and organizational roles. Software platforms allow collect and storage of information from devices, data correlation, and display of appropriate information for people with each role in the process and facilitate information exchange between roles for assuring optimal delivery of communication services. Any management tool will be of little value if it is not integrated into an appropriate management process.

Figure 2 presents some major tasks performed in an operational telecom network. These tasks are classified as Service Fulfilment (setting up of connections and services), Service Assurance (assuring the delivery of adequate services), and Service Support (maintaining the service and the network infrastructure). The tasks are further classified as User-facing (service customer related), Network-facing (resource and infrastructure related), and service-related translating customer requirements into service connectivity objectives to be fulfilled using network resources.

	SERVICE FULFILMENT (SETTING UP)	SERVICE ASSURANCE (ASSURING DELIVERY)	SERVICE SUPPORT (MAINTAINING)
User-Facing	User Order Handling User Change Handling User Inventory	User Problem Handling User SLA Management Customer Relationship Mgt	Service Enquiry Desk (User Technical Support)
Communication Service	Service Provisioning, Config. & Activation Service Inventory	Service Incident Management Service Quality Management Service Impact Analysis	Service Change Management
Network-Facing	Resource Provisioning Network Inventory	Network Fault Management Network Root Cause Analysis & Problem Management. Network Perf. Monitoring	Net. Config. & Change Mgt Network Maintenance Mgt Asset Lifecycle & Spare Mgt Platform & Tools Support

Figure 2- Telecom Network Operation tasks of Service Fulfilment, Assurance and Support for a dedicated infrastructure operational telecom network

Executing management tasks requires real-time knowledge of the network's current state – a snapshot of faults and performance of the network, and a knowledge of the network configuration through a network data inventory – providing a context to real-time information and correlating different real-time event data.

A typical operational telecom management model is presented in figure 3 hereafter. It distinguishes the following roles:

- Network supervisor assuring the health and proper performance of the network,
- Service manager assuring that "user service" commitments are met,
- Maintenance & Support engineers in charge of incident resolution and configuration change,
- Network Planner deciding upon modifications, adjustments, and extensions of the network.

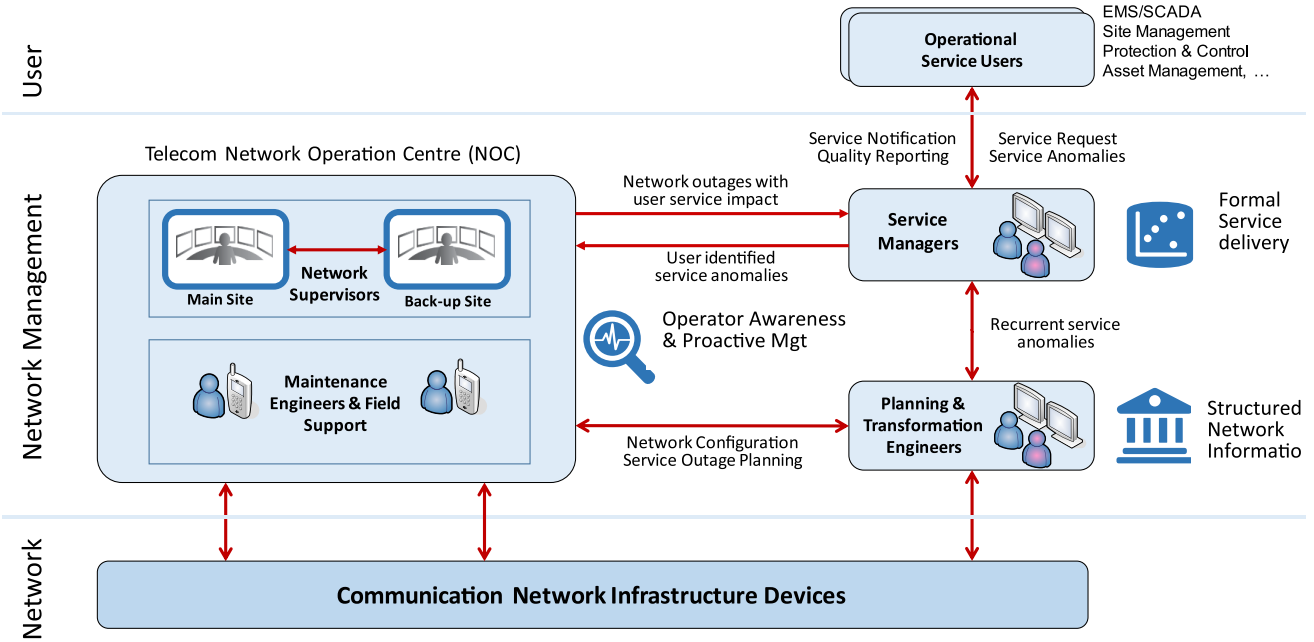


Figure 3 - Management of operational telecom network and services

2.2. NETWORK MANAGEMENT: FUNCTIONAL DOMAINS AND FUNCTIONAL LAYERS

Conventionally, the management of the communication network is partitioned into the following functional domains:

- **Fault Management** consists of detection and localization of network faults mainly through collection and analysis of device alarms but also through detection of performance anomalies. It comprises also the determination of service impacts of network faults and notification of impacted users. **Incident management** is closely related to fault management, comprising incident ticket opening, assignment of its resolution to the appropriate team or person and its follow-up to the elimination of the anomaly and the closure of the ticket.
- **Configuration Management** is a wide domain of functions. It includes the network inventory maintaining information on network devices, connections and delivered services. It also covers the capability to discover configurations and settings from field-installed devices, and the capability to change them for adapting network resources to service requirements.
- **Accounting Management** concerns the determination and policing of network resource usage, and billing of services for each group of users in a multi-tenancy network. Even if services are not truly billed in most operational networks, it becomes increasingly necessary in most Utilities to have awareness of the extent of resources used by each user application.
- **Performance Management** consists in monitoring pre-defined network/service metrics to assure that the quality of the delivered service matches the agreed level (Service Level Agreement, SLA) and to signal any operational anomaly to the fault management function. The most basic performance to monitor is indeed the downtime (or availability) but in the packet-switched context, it equally covers throughput, packet loss and delay (absolute delay, and delay variation). Performance monitoring comprises "threshold crossing alarms" for network anomaly detection, and statistical analysis for long term SLA management.
- **Security Management** is also a wide concept covering the whole information processing and exchange chain. For the communication network, it consists of not degrading in the "Wide Area", the security of information (Confidentiality, Integrity, and Availability) achieved in the "Local Area". In this context it covers the protection mechanisms in place for role-based access control to devices and to the management platforms (e.g. RBAC) as well as the proper isolation of logical connections and services across the network.

Network management is also partitioned into 4 functional layers:

- Element Management manages each individual network device,
- Network Management concerns end-to-end connectivity,
- Service Management concerns User Services and expectations (Service Level Agreements),
- Business Management (in the operational context) concerns service planning and transformations for optimal usage of resources and preserving investments in the network.

Figure 4 presents the interaction between the above-described domains and layers. This conceptual model is essential for appreciating the advantages and shortcomings of device-specific and device-agnostic management tools and the way they can be associated for optimal operational capabilities.

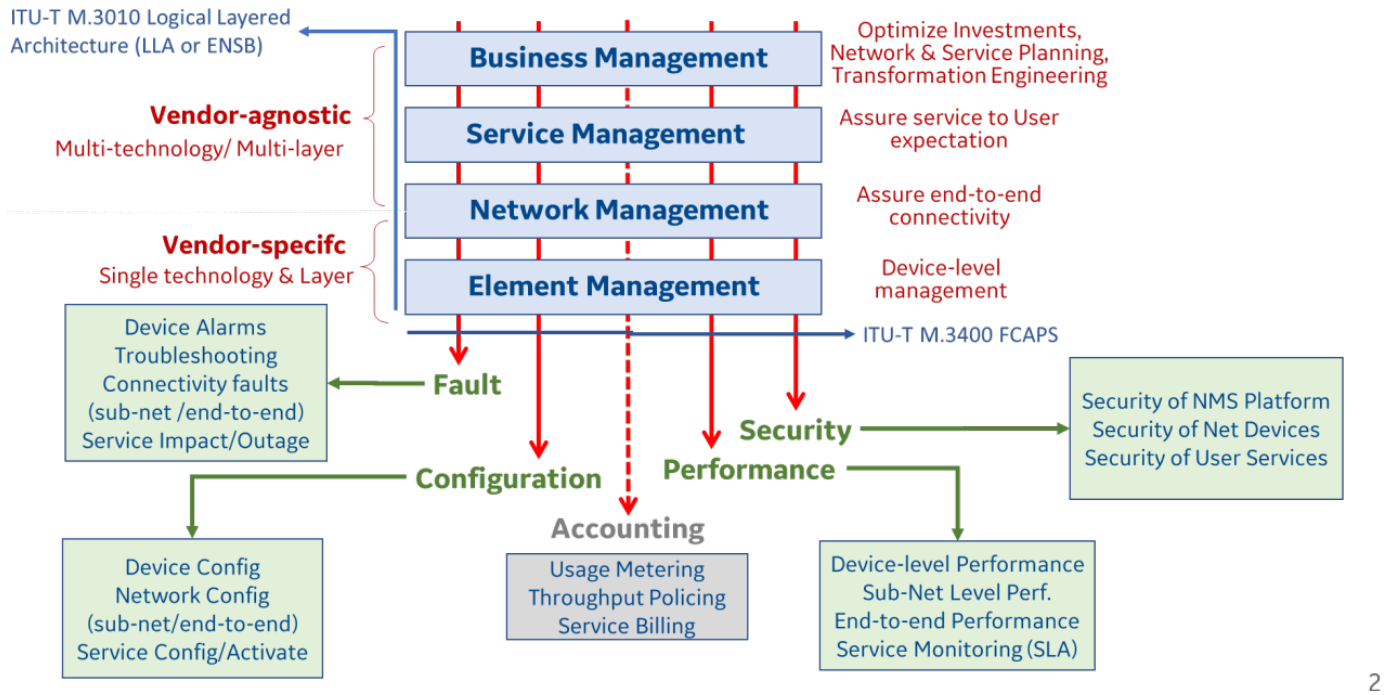


Figure 4 – Network management functional domains and layers

2.3. LAYERING THE NETWORK MODEL FOR MANAGEMENT

Operational telecom networks are generally composed of multiple layers of connectivity, starting at the bottom with physical connections over fibers, wireless or electrical conductors, then transported as logical connections over packets, circuits, or any combination such as Ethernet over SDH, Circuit Emulation over Packet, MPLS Pseudowires, etc., for finally delivering different types of connectivity service for user applications. Each connection at one layer requires the proper operation of some connection resources at underlying layers. Modeling the network through "dependency relations" between layers of infrastructure allows to perform Root Cause and Service Impact Analysis on the network. Dependency relations are maintained in the network inventory of the central management framework.

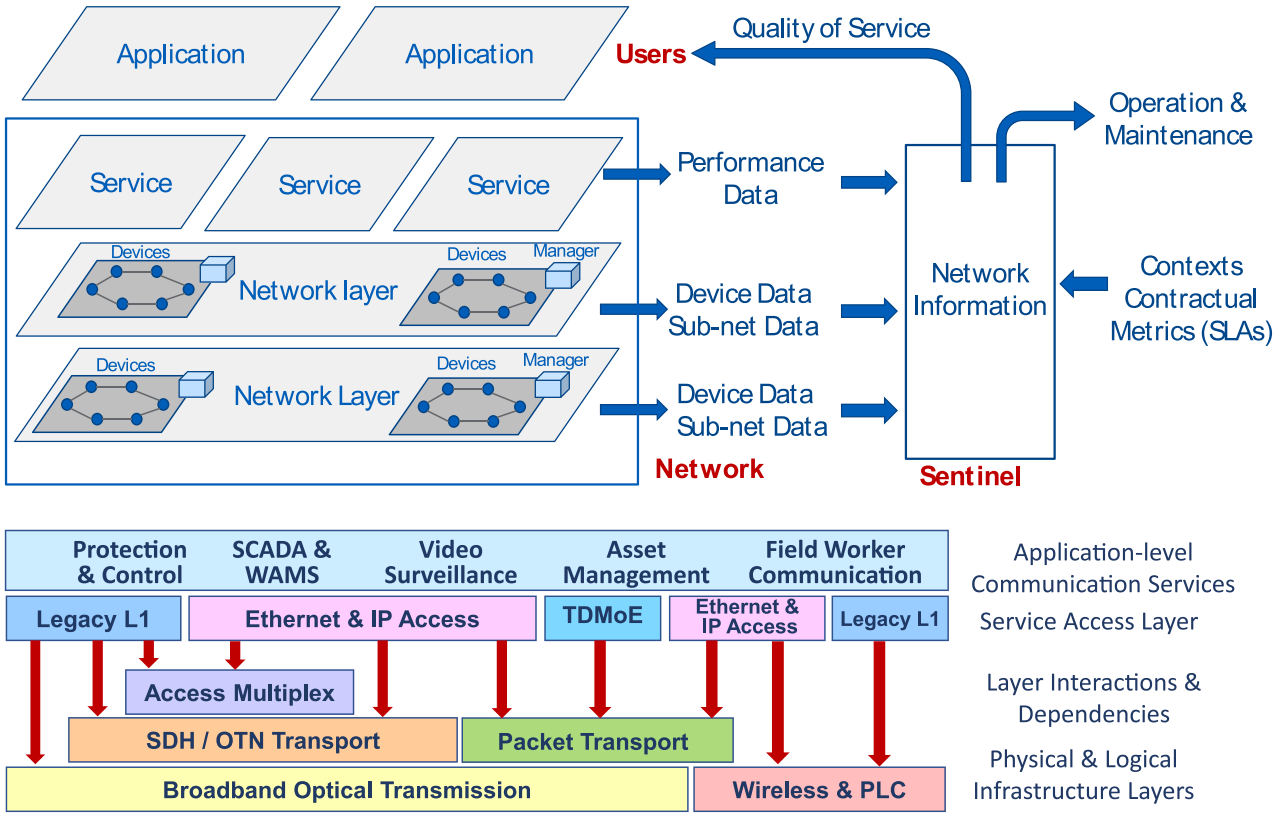


Figure 5 – Multi-Layer Network Modeling

2.4. IMPLEMENTING THE MANAGEMENT SYSTEM

Network data can be stored in one or multiple tables or maps, and network supervision may be performed using one or multiple device-specific Network Management Systems, as historically performed by all (and still performed by some) Utilities. The Management platform is here composed of several distinct vendor-specific tools as presented in figure 6b, together with some form of off-line documentation system maintaining all data on devices, network interconnections and communication services. Device-specific management systems constitute essential tools for configuring, commissioning, and troubleshooting a single vendor's sub-network.

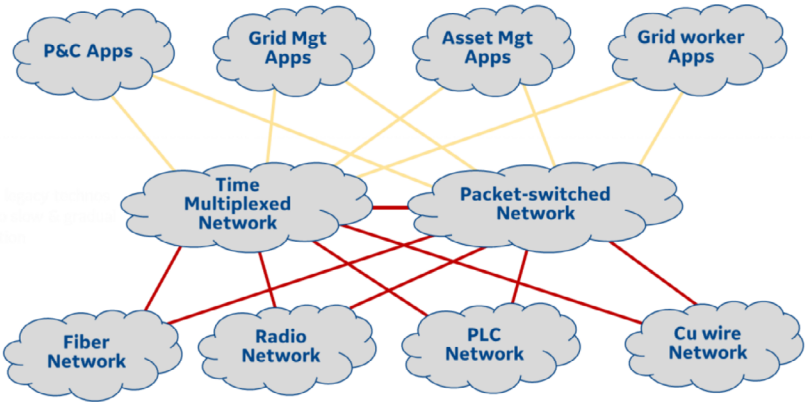


Figure 6a – Telecom network using Time-multiplexed and Packet-switched technologies to deliver operational services over fiber, wireless, PLC and wire infrastructures

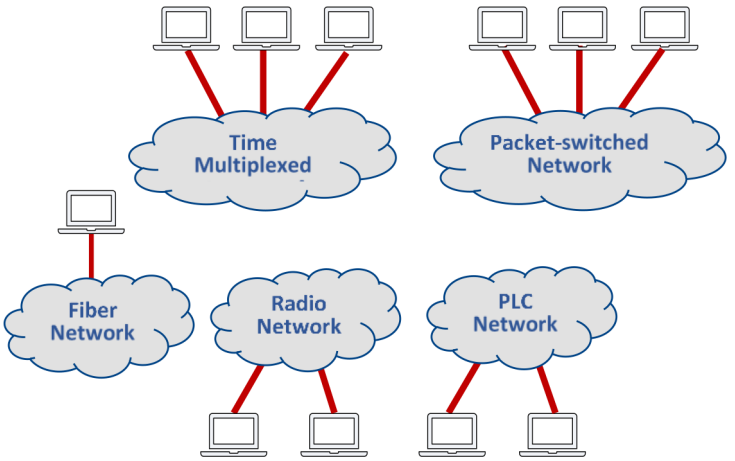


Figure 6b – "Siloed" Management through Vendor-specific Management Systems

However, for large and complex networks, such an arrangement is no longer adequate. It does not give a full situational picture of the whole network facing an avalanche of alarms: for example, information from different sub-systems cannot be correlated to determine the root cause of network anomalies or the consequences of network faults on delivered services.

Moreover, as the management tools are fully independent of each other, there shall be no information coordination across the network, and therefore no possibility of higher-level applications for optimizing network resource usage or visualizing resources allocated to an end-to-end service.

There exist essentially two approaches for assuring a federated management of all network assets and services:

1. Replacing all vendor-specific management systems by a single management system connecting to all devices and collecting information from the whole network. This approach, rendered possible through standard protocols such as SNMP, allows network faults to be monitored centrally and building some statistics. However, the approach is less practical for device configuration and detailed diagnostics, requiring detailed device models and extensive work at each introduction of a new device type.
2. Use vendor-specific management systems as "mediation gateways" connecting to each family of equipment and delivering management capabilities to a central framework. This "Manager of Managers" or "Umbrella" approach requires access from the central platform to each NMS using a Northbound API (Application Programming Interface). At present, Northbound APIs available on vendor NMS platforms are often limited to SNMP alarm indications, even if more functionalities through a REST API are planned in many product roadmaps. A simplified alternative here is to open relevant NMS windows from the central framework and hence manipulate centrally the dedicated management systems.

GE Vernova Sentinel system presented in the following sections has adopted a combination of these approaches – direct device fault management through SNMP and diagnostics/setting/provisioning through vendor-specific management systems accessed by operators through the central framework.

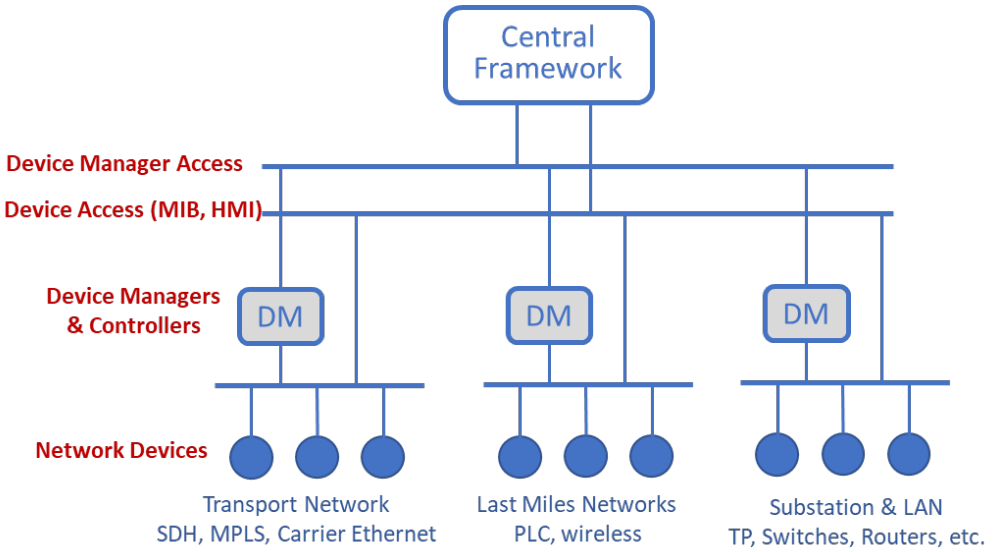


Figure 7 – Central Framework access to network devices. Device Managers are manually opened as separate windows

2.5. PACKET-SWITCHED NETWORK MANAGEMENT

Grid digitalization is transforming operational communications gradually converging to IP/Ethernet for all substation applications (Protection & Control, Control platform data access, workforce facilities, etc.) moving the activity focus from physical interface and cable coordination to network coordination. Network implementation and operation become less laborious, due to fewer cables and interfaces, but more complex to design and to maintain, because of the virtuality of connections. The supervision system but document and identify – beyond the device – logical ports and virtual connections At the same time, operational communication network technology is rapidly migrating to packet switching both at access level (Ethernet service aggregation) and at transport level (large-scale packet-switched MPLS core transport).

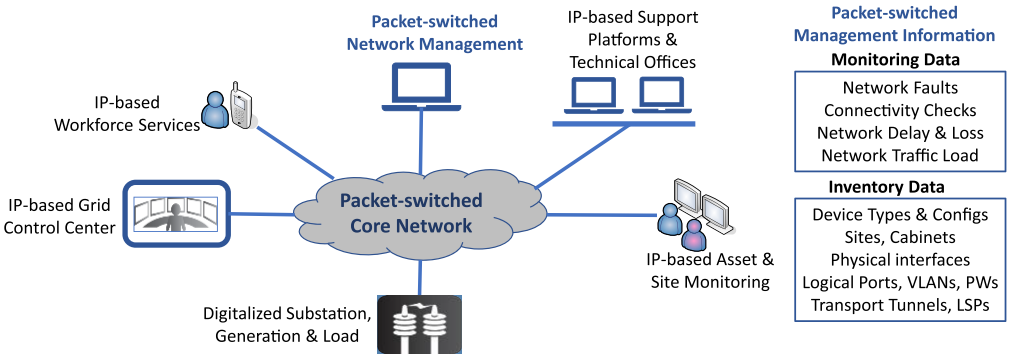
Packet-switching considerably enhances network efficiency through resource sharing. However, it also impacts the behavior of the delivered communication services, potentially causing variable delay, data packet loss, path uncertainties and security issues. Network anomalies, mainly caused by device failure in the legacy SDH/SONET network, are dominantly related, in the packet-switched network paradigm, to unsatisfactory performance. Performance monitoring is therefore a major function in the new network: resource sharing and packet routing need to be monitored and remotely controlled to adapt to topology and network load changes, as well as the detection of performance-related anomalies.

Moreover, connectivity across the network, easily monitored in SDH/SONET networks becomes difficult to monitor in packet-switched networks due to their non-persistent connections. There is a need for periodic exchange of extra messages to check the viability of communications. Standard mechanisms are available for connectivity monitoring for some packet technologies but need adequate settings to be exploited in an intelligent manner.

Finally, the packet-switched network paradigm transforms the automated provisioning issue, a long-time desire of operational telecom operators, into that of creating and managing Ethernet Virtual Connections (EVC), VLANs, Label Switched Paths, and Pseudo-wires.

Many of these capabilities are existing as standard functions of network devices exploited through corresponding management tools. The problem to solve is to assure coherence between the real network and its “digital twin”, the connected network inventory.

Complexity, lack of situational awareness, and lack of control are obstacles to the migration towards new generation networking. These issues can be largely overcome through a powerful management platform, a major asset for reliable operation of packet-based networks.



TDM NETWORK (SDH/PDH)	PACKET-SWITCHED NETWORK (ETHERNET/MPLS)	
Permanent and continuously monitored connections with largely constant performance. Anomalies are mainly detected at commissioning or due to device faults during operation.	**Store-and-forward** with intermediate **queuing**. Anomalies may appear during operation due to changing load, path change, priority table updates, etc. Must also **check connectivity** through specific message exchanges (OAM-PDUs)	Need to monitor network values and detect changes. Collected data to be processed through statistical models **(Statistics engine)**
Alarms during operation mainly due to device faults.	Alarms during operation mainly due to **threshold crossing.**	**Threshold Crossing Alarms** (at device and at network-level)
Every Service corresponds to a distinct Physical interface.	Services are associated to **logical ports**	Use **Network Inventory** and associated research functions for identifying logical ports associated to a Service

Figure 8 – Packet-switched Operational Network paradigm

3. MANAGING OPERATIONAL NETWORK USING SENTINEL

Sentinel is a service-centric management platform associating real-time monitoring and incident management with a network inventory that structures network data into an overlay model. It is a major step forward in providing enhanced awareness on the network and on delivered communication services. Major capabilities and functional enhancements are highlighted below and further discussed in the following sections.

1. **Web-based User Interface** – An advanced template-based user interface together with customized data restitution settings cover all functions in a standard manner as commonly used to create interactive web-based applications. This web-UI replaces the previous proprietary presentation framework.
2. **Network Inventory** – Sentinel incorporates an enhanced physical/logical inventory storing "overlay-structured" information for supervised and non-supervised network devices and their interactions. The network inventory provides the base for fault identification (root cause analysis) and impact analysis, as well as for managing bandwidth usage and network transformations. Devices, connections, and user services can bear additional data on ports, interfaces, virtual connections, capacity, shelves, serial numbers, firmware release, etc.
3. **Alarm Management and Network-aware Fault Supervision** – Sentinel collects alarms and events from devices into a real-time supervision database. Alarm information is collected through SNMP either natively from the device, using alarm contacts of the device through an SNMP converter, or using the SNMP Northbound Interface of a Device Manager/dedicated NMS. Sentinel performs alarm management functions such as filtering by time window, by type, or by zone. It associates received events with inventory data to produce layered network maps presenting devices, connections, and user services together with their status as a color code. Furthermore, Sentinel combine inventory-stored relations to estimate connection outages and propagate the impact on other layers according to pre-defined dependency relations.
   - **Root Cause Analysis** function allows to correlate higher layer (service) faults with any underlying connectivity faults in the network.
   - **Service Impact Analysis** function allows to return all connection services being transported over a selected unavailable segment.
4. **Incident Management and Problem Resolution** – Sentinel enables creation of incident tickets identifying concerned network resources, provides device and connection types, configuration, and history, to assist with problem resolution, allows resolution task assignment to appropriate operation staff, enables incident follow-up, and stores succinct resolution reports. Upon incident closure, Sentinel estimates incident resolution time and occurrence statistics. Moreover, the platform allows network actors (user, service manager, supervisor, maintenance, and transformation) to exchange operational messages through a Whiteboard.

5. **Performance Monitoring** – Sentinel estimates service availabilities and downtime distributions using device alarms and dependency relationships, generating service dashboards for each group of services and connections. Moreover, Sentinel can periodically collect pre-determined performance values (e.g. traffic load on a given port of a given device) stored in network device MIBs, according to preset "monitor points". The settings determine the location of the monitored value, frequency of data collection, and collected data handling (Excel file dump for off-line analysis, statistical model-based predictive analysis, etc.).

6. **Configuration Management** Configuration management functions in Sentinel are focused on the Network Inventory "digital twin", or by providing a framework for remote connection to device HMI and specific device managers:

   - **Path Tracking** – allows to trace the path taken by a connection across underlying network.
   - **Bandwidth Management** – allows to estimate used/spare capacity of a connection by comparing its capacity with the inventory-stored bandwidth of all overlaying services.
   - **Work-order preparation** for network transformations, deployments, and service provisioning – allows to create the "digital twin" of the resources and connections before they are implemented on the actual network. This can serve as a work-order for the works to be undertaken.
   - **Device diagnostics, configuration, and control** – Sentinel provides a framework allowing a point of access for device HMI and vendor-specific Network Management Systems without costly, complex, and often out-of-reach integrations. Device HMI ports and vendor-specific NMS or Device Controllers may be accessed through Sentinel framework through right-clicking of assets on Sentinel displays. Separate windows on device-specific tools are opened for these tasks via Sentinel User interface. This approach can be implemented easily for almost any type of device without the need to develop device-specific interface adapter software. It remains an adequate and cost-effective solution for operational networks.

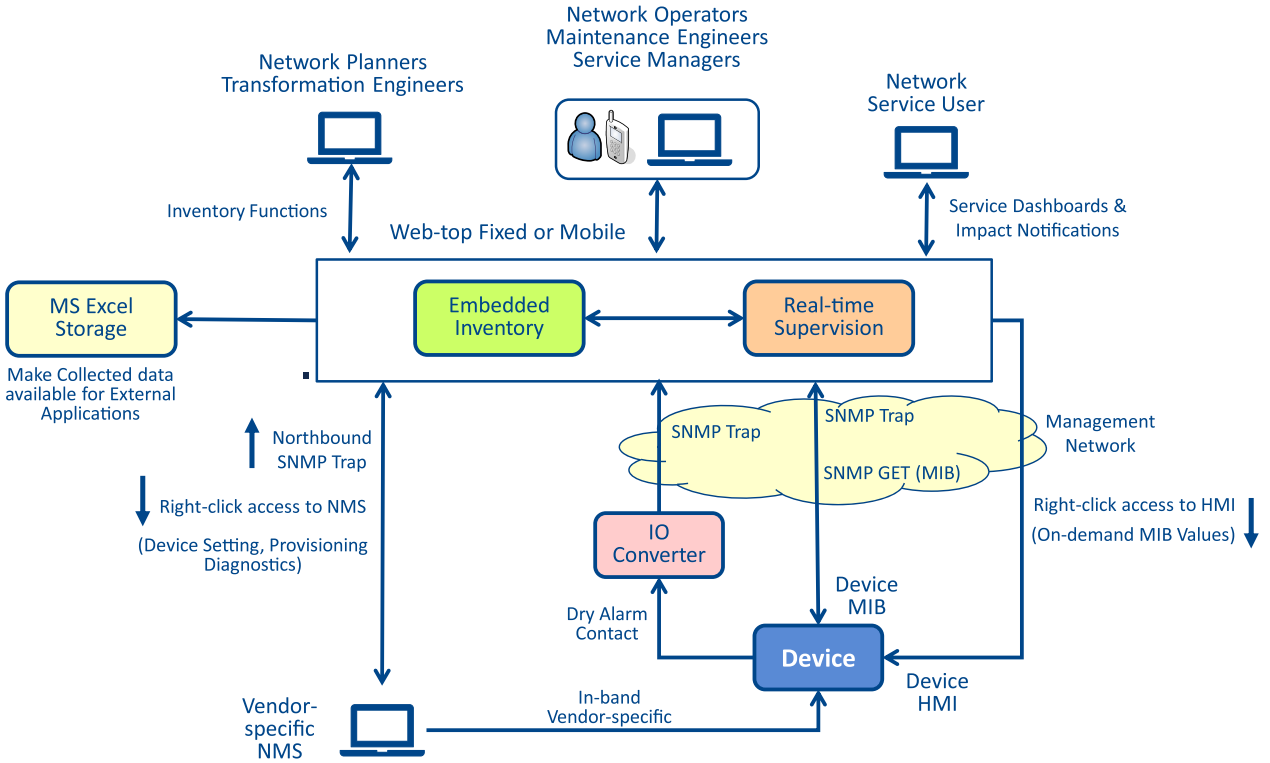


Figure 9a – Sentinel data exchange architecture

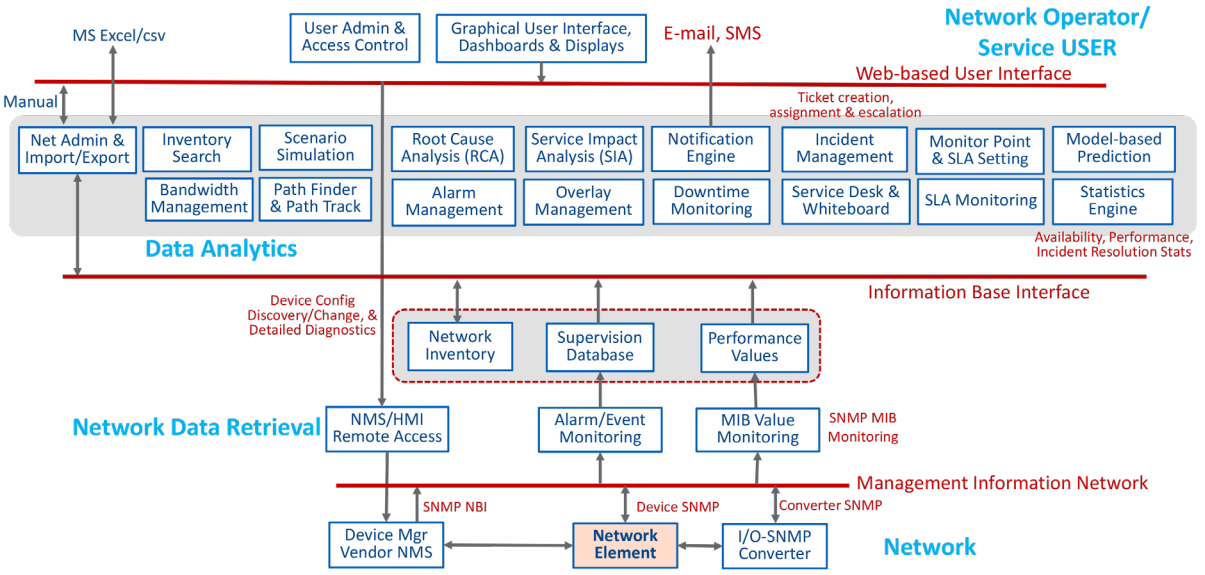


Figure 9b – Sentinel functional architecture

4. NETWORK INVENTORY – NETWORK-AWARE MANAGEMENT

Structured information on devices, connections and dependency relations in a data inventory is an important constituent of the management process. Collected real-time network data is given a network context by the inventory, without which it would be reduced to a "flat event list". This is used for investigating network faults in the problem resolution process where the inventory provides a reference image of network and its devices and their interactions.

Network inventory can also be used independently from real-time supervision and can be associated to non-supervised nodes to maintain a full picture. Configuration and device data may be used for planning of network transformations and extensions. They must be up-to-date and correspond to both engineering and field reality. Sentinel stores network site, device, and service data as well as information on network connections and inter-layer dependencies.

Sentinel 4.0 structures these data into a full-scale network inventory with port information associating services to devices, and several inventory-based search applications as described in the following sections. The communication network inventory data are summarized below:

Device data	Device type, site, network layer, owner, and IP address. Additional attributes such as device configuration, cubicles, serial numbers, etc. may be added (meta-data) for a given asset type, without any specific development. Moreover, Sentinel 4.0 allows the addition of physical interfaces according to pre-defined interface types for each type of device. Physical interfaces support Logical Ports which are associated to transported services.
Network data	Physical and logical connections between devices with main & alternate paths and layer dependencies. Logical ports can bear information on VLANs and pseudowires associated to each service, mapping them with devices.
Services and SLAs	Service Inventory – list of services and their attributes (layer, end-point devices and ports, bandwidths, ...). SLAs are agreed Quality limits for each service type, whose monitoring allow to prove the delivered service meets contractual requirements.

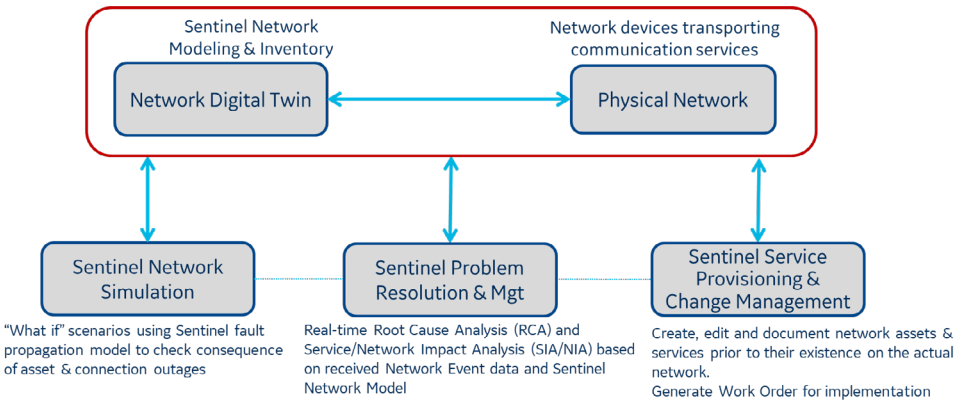


Figure 10 - Sentinel Inventory as a Network "Digital Twin"

4.1. DEVICE, INTERFACE, PORT, AND SERVICE

Supplementary information fields for devices and services can be added and used according to network operator's specific requirements. Some typical examples of this asset/device meta-data usage are presented in figures 11a and 11b below.

ASSET CLASS	CLASS-DATA1	CLASS-DATA2
TP Signaling	Hardware Configuration	Hardware version / Firmware Release
Scada RTU	Hardware Configuration	Hardware version / Firmware Release
Voice PABX	Hardware Configuration	Hardware version / Firmware Release
Access MUX	Hardware Configuration	Hardware version / Firmware Release
Ethernet Switch	Hardware Configuration	Hardware version / Firmware Release
MPLS-TP/CE Switch	Hardware Configuration (10G, GbE, STM1, E1, FE)	Hardware version / Firmware Release
PLC Terminal	Tx Freq; Rx Freq Coupling (PE, PP, IC), Line Trap value	Hardware version / Firmware Release
SDH Add-Drop	Hardware Configuration (STM16, STM4, STM1, E1, Eth)	Hardware version / Firmware Release

Figure 11a – Some examples of Asset (Device) additional data field usage.

Hardware configuration example: 1CPU+2PS+2x Type A interface + 2xType B interface (for PLC we have adopted in this example Transmit/ Receive Frequency bands, line coupling type and Line Trap inductance(mH) as Class-Data1

SERVICE LAYER	SERVICE TYPE	BANDWIDTH/CAPACITY	DATA1	DATA2
NMS	Server/WS/NMS/ IO Conv	GbE/FE/ETH	Mgt. Network Protocol	
Teleprotection	Analog/Coded/ETH	Analog/Sub-E1/ E1/ NxE1/ETH	Link Protection Mode	
Scada	RTU/ICC/WS	Sub64/subE1/E1/ETH	Network Protocol (IEC101/104/ICCP/ DNP3)	
Voice	VoIP/CCS/CAS	E1/subE1/Analog	Network Protocol FXO/FXS/E&M/ DPNSS	
PDH Access	nE1oSDH/nE1oPDH/TDMoP	NxE1/E1/sub-E1		
WAN Tunnels	MPLS-LSP / Nat. ETH/ EoS	Sub-E1/E1/NxE1/FE	Protection Mode (G8032/G8031/STP)	CIR: xMbps/PIR: yMbps
PSN Backbone	MPLS-TP/CE/ETH	10GE/GbE/FE/ETH	Protection Mode	Distance (km)
Power Line Carrier	Analog/Digital/Hybrid	PLC link BW (8+8 kHz)	Line Voltage (kV)	Distance (km)
SDH	e.g. Fiber/1550/LR	STM-16/-4/-1	Protection Mode (e.g. SNCP/MSP)	Distance (km)

Figure 11b - Some Examples of usage for Service attributes and additional data fields

Sentinel 4.0 Network Inventory is further enriched with physical and logical interfaces. It is not mandatory to fill interface and port information for devices: a simple system can be built with minimal elements – Asset (device) and Service (connections) and then gradually enriched with further elements such as Physical Interfaces on devices, and Ports identifying the association of the interfaces with their usage for transporting services. Ports may be used to identify VLANs, Label-switched Paths and Pseudowires in packet-switched connections, and channels on an interface board (circuit-to-service association) for circuit-based connections.

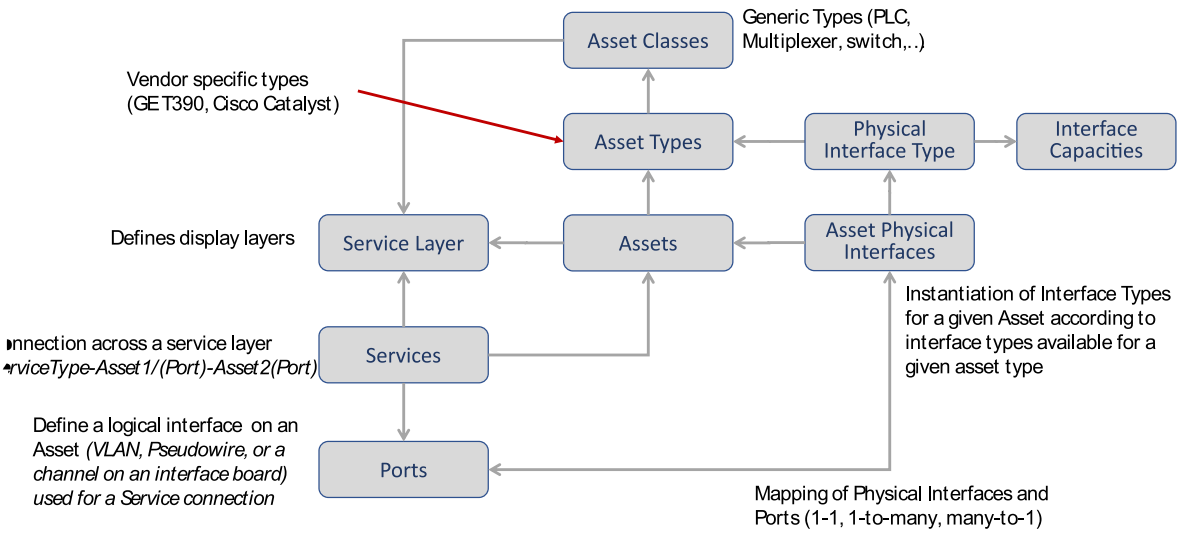


Figure 12 – Asset, Interface, Port, and Service relations. Arrows indicate sense of attributes, for example a Service Layer must be defined before defining a service which will use it as an attribute.

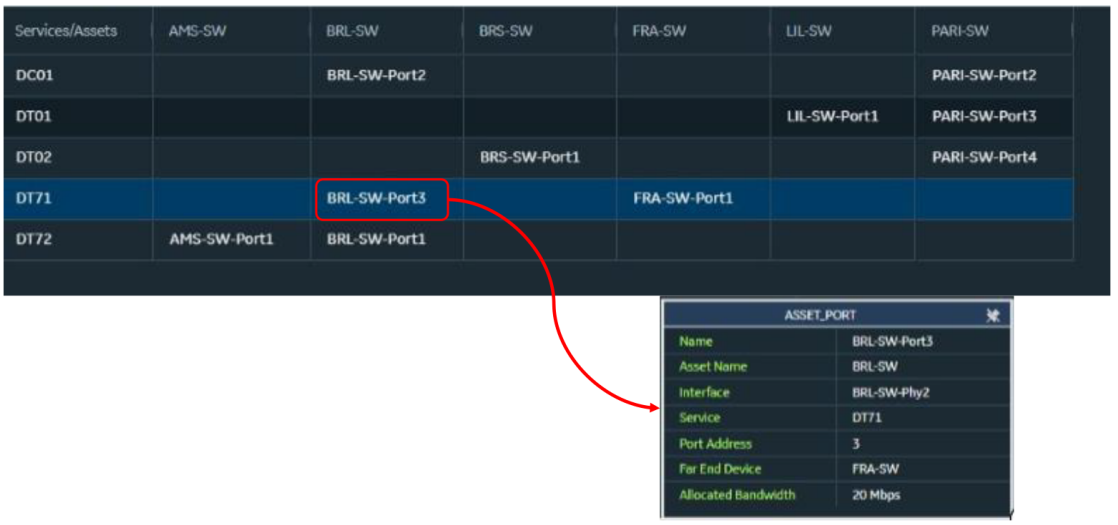


Figure 13 – Port identification on Switch devices and their Physical interface allocation. Data service DT71 in this example connects Ethernet switch at site Berlin (BRL-SW) on Port 3 to Ethernet Switch at site Frankfort (FRA-SW) on Port 1. Logical Port 3 of Berlin switch resides on Physical interface 2 (BRL-SW-Phy2) with its far end interface at FRA-SW and with an allocated bandwidth of 20Mbps. Further information on this physical interface and on each of the devices may be searched in the inventory base (shelf reference, device type, configuration, ...)

5. NETWORK FAULT MANAGEMENT, RCA AND SIA

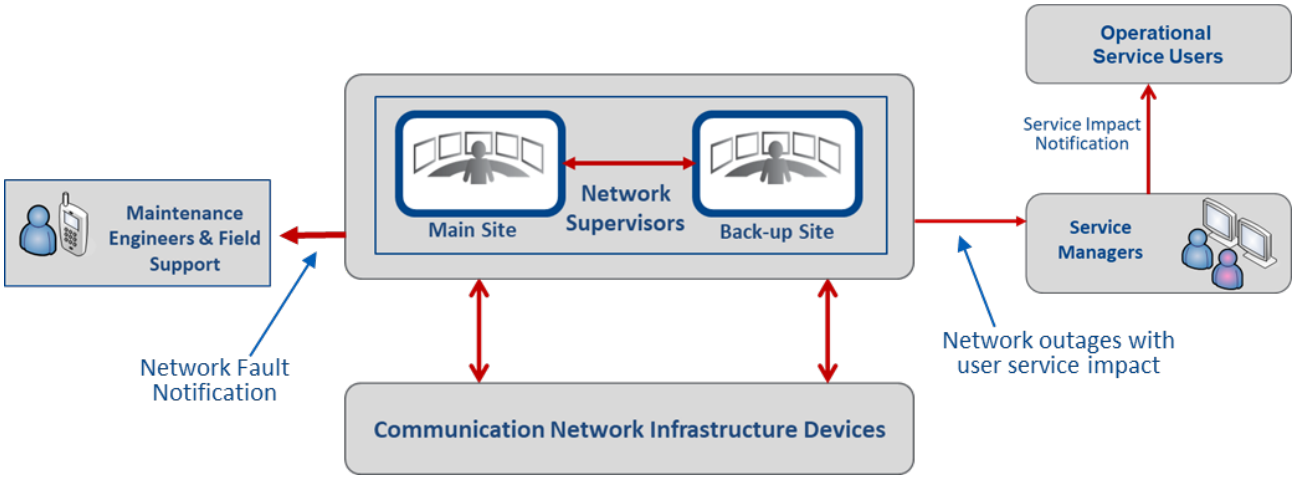
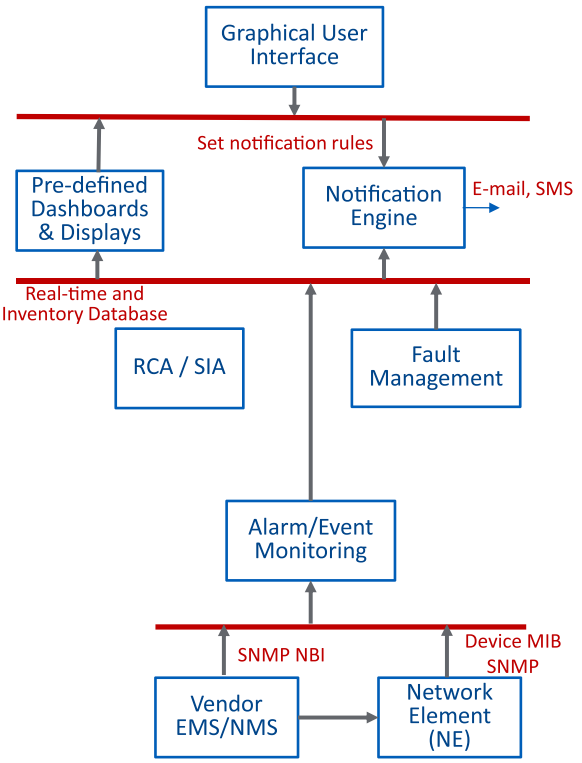


Figure 14 – Actors of a Fault Management Process

Device alarms are transmitted as SNMP traps to the fault supervision platform and used for detecting network connection faults. Faults and anomalies can also be detected by the operational service users and transmitted as a "Service Anomaly" message. The process is as follows:

1. Network Element, I/O converter, or Vendor NMS transmits SNMP Trap upon alarm condition.
2. Alarm/Event Monitoring receives the SNMP Trap.
3. Event is associated to a device with pre-defined severity.
4. Device is mapped to a Functional Layer and to a sub-network as recorded in the Network Inventory.
5. On the functional layer supervision display, device changes status according to event/alarm.
6. All connections on the device change status according to alarm status on the other termination device.
7. Connection status propagates into overlaying layers of network and service according to pre-defined dependency relationships.
8. Event/alarm conditions are used to generate notifications according to custom defined rules and notification messages are transmitted to pre-defined actors and service users.
9. Active device alarms are displayed by functional layer and by geographical zone on the supervision map. Number of connection services which are available, unavailable/impacted are also displayed on the Fault Dashboard.



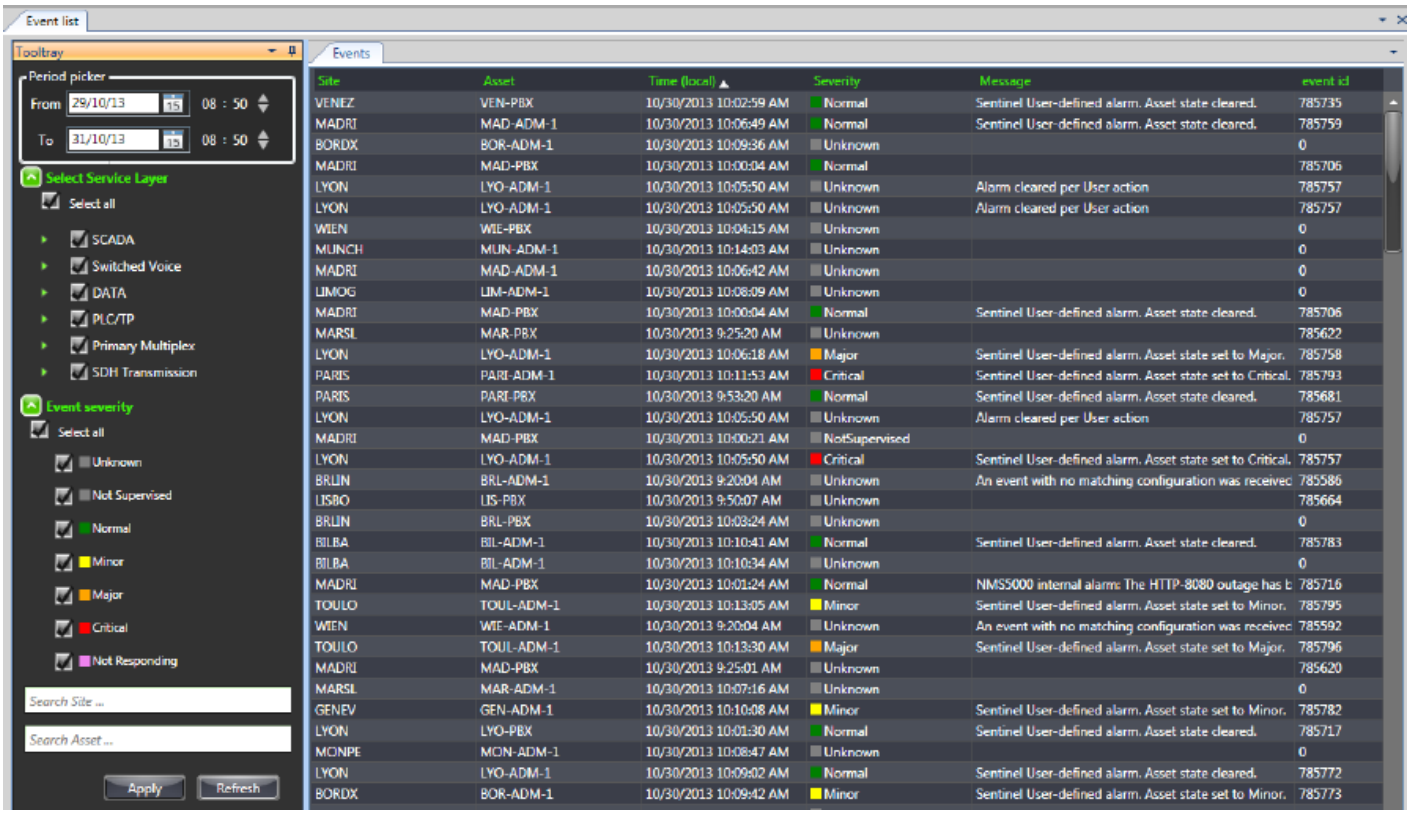


Figure 15 - Sentinel Fault Management - Event List

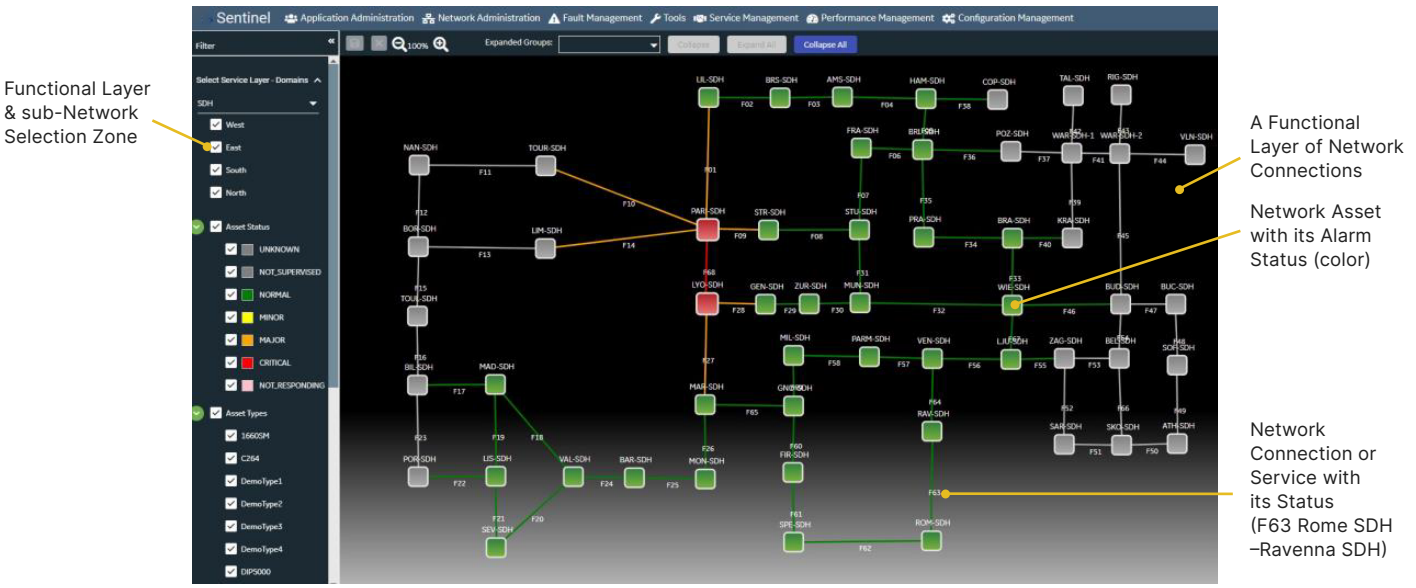


Figure 16 - Sentinel Fault Supervision Graphical Display

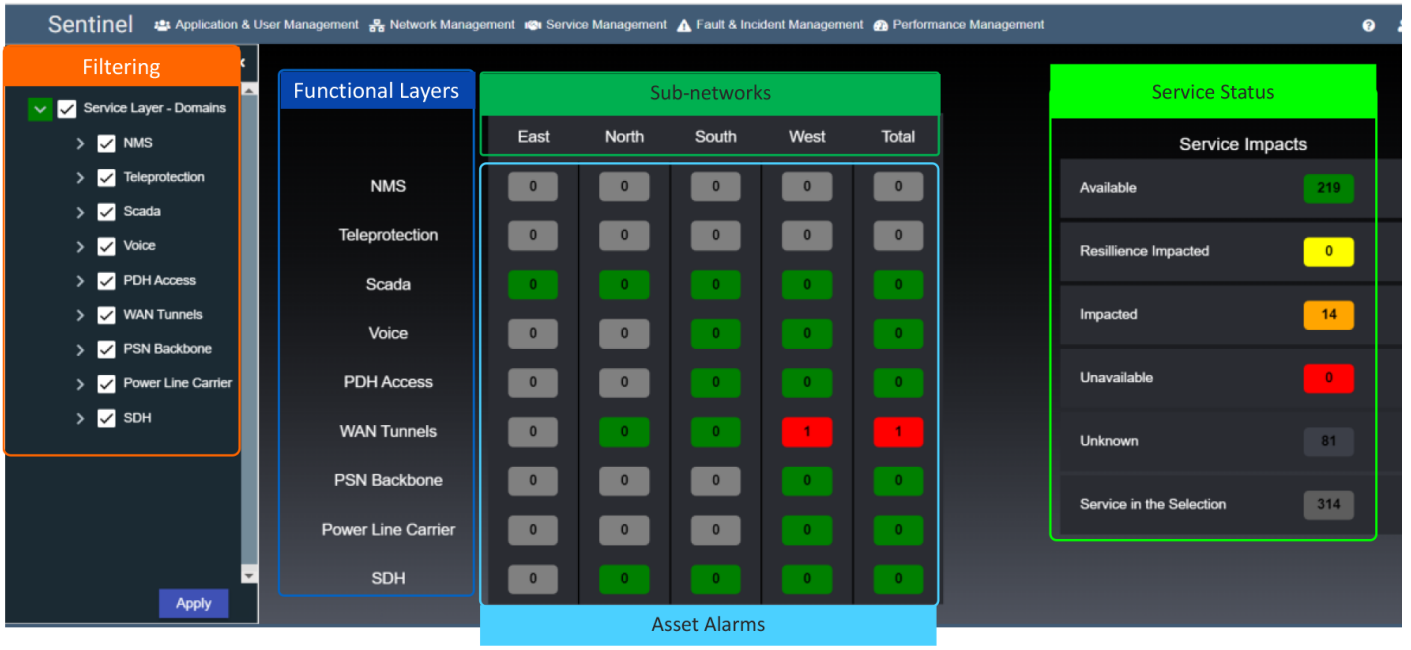


Figure 17 – Aggregate Fault Dashboard presenting Device Alarms and Service Status

5.1. DETERMINING FAULT CAUSE AND CONSEQUENCES - RCA & SIA

Root Cause Analysis (RCA) and Service Impact Analysis (SIA) are two essential components of operational problem handling. RCA determines the network cause of a service failure by digging into the underlying infrastructure through dependency relations. It allows the identification of the origin of an avalanche of correlated fault indications. SIA, on the other side, allows the identification of all overlaying services and connections which may be impacted by the consequence of a fault in the underlying infrastructure (e.g. all the services which are impacted by the outage of a given transmission segment).

5.2. ROOT CAUSE ANALYSIS (RCA)

A Service ID is selected and the system returns the Main or Alternate underlying connections, indicating the status of the selected service as well as those of underlying connections and devices through color codes. This allows to determine the root cause for the unavailability of the selected service.

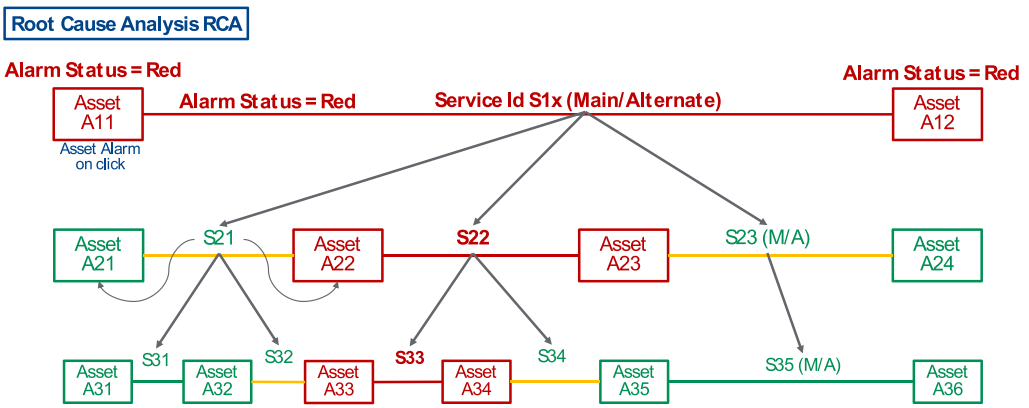


Figure 18 – Root Cause Analysis principles – Service S1x connecting (A11, A12) is in alarm. S1x depends upon services (S21, S22, S23) connecting Assets (A21, A22, A23, A24), which in turn depend on services (S31 .. S35) connecting assets (A31 .. A36). Considering the status of respective devices (assets) it can be observed that the root cause for outage of service S1x is a fault on S33.

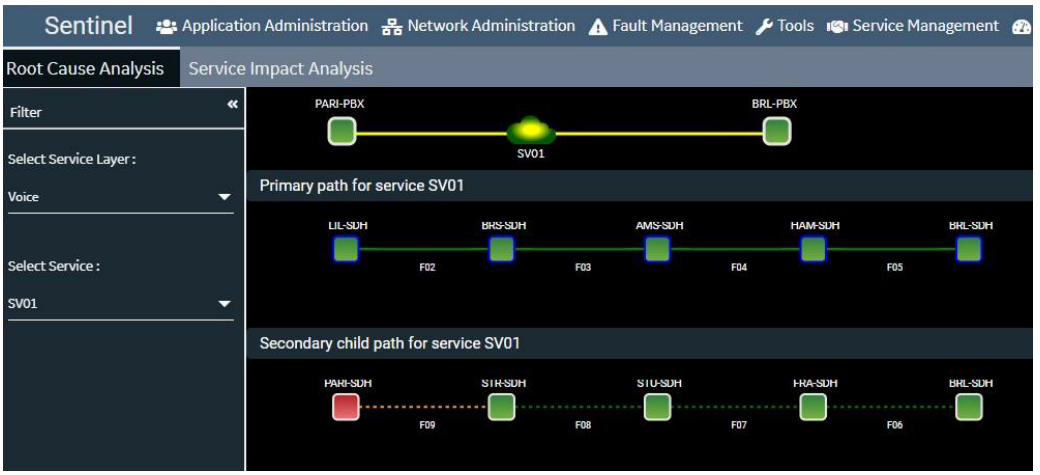


Figure 19 – Root Cause analysis display in Sentinel

5.3. SERVICE/NETWORK IMPACT ANALYSIS (SIA)

As illustrated in figure 19, the system returns all services using a faulty network connection (Service ID S1x) in their Main or Alternate paths as illustrated in figures 20 and 21.

	Layer	Service Id	Main	Alt	End Asset A	End Asset B
Analyzed Service	X	S1x			AX1	AX2
Impacted Service	Y1	Sy1 (Main)	Y	N		
Impacted Service	Y2	Sy2	Y	Y		
Impacted Service	Y3	Sy3	N	Y		
Impacted Service						
Impacted Service	YN	Syn	Y	-	AN1	AN2

Figure 20 – Service and Network Impact Analysis in Sentinel

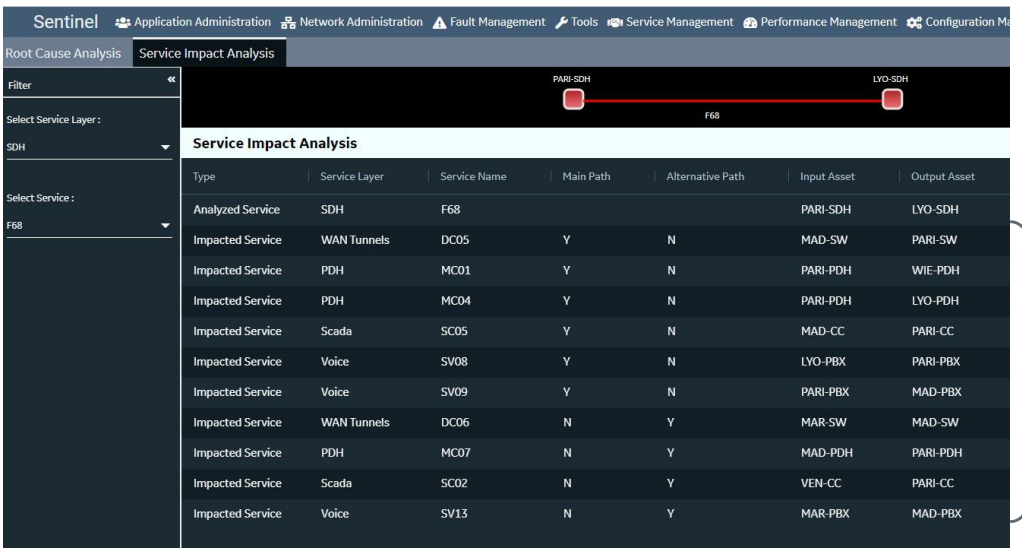
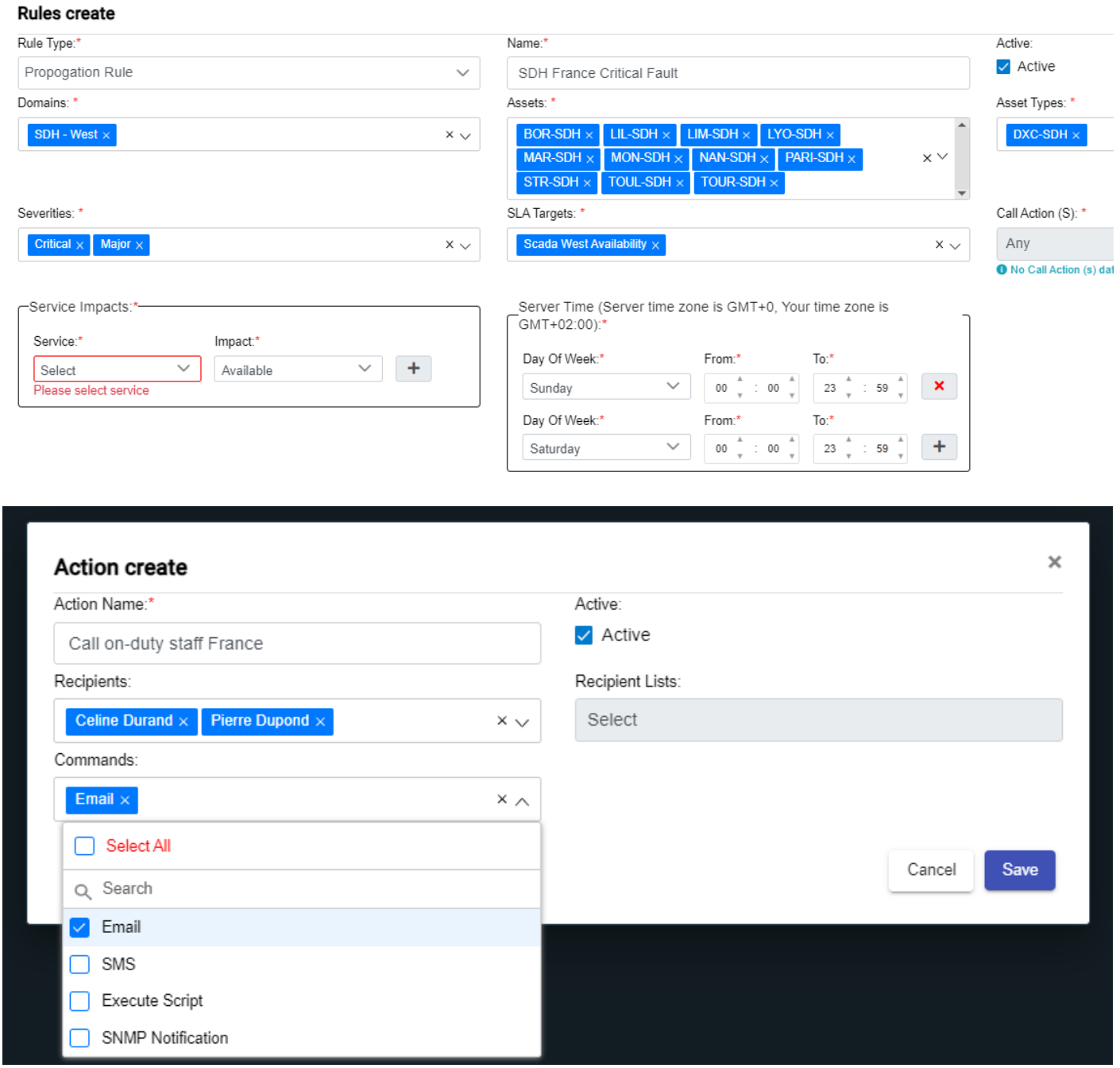


Figure 21 – Service Impact Analysis display in Sentinel

5.4. THE NOTIFICATION ENGINE

Sentinel includes an Alert Notification function that allows to take automatic actions upon detecting a pre-determined triggering condition. Automated actions comprise sending an e-mail or an SMS message to a pre-defined recipient (Operation & Maintenance actor or Service User), generating an SNMP Trap message towards a higher-level external management platform or Sentinel Event-management database, or executing any user-defined script. Triggering conditions are defined as "Notification Rules" comprising a combination of Asset events and severity, SLA Target limit detection, and time of day defined for each day of the week (e.g. Sundays all day, and week days out of office hours, send an SNMP Trap to Control Center platform, or an SMS message to the on-duty maintenance engineer).



Sentinel Notification Rule and Action initialization

6. INCIDENT MANAGEMENT & PROBLEM RESOLUTION

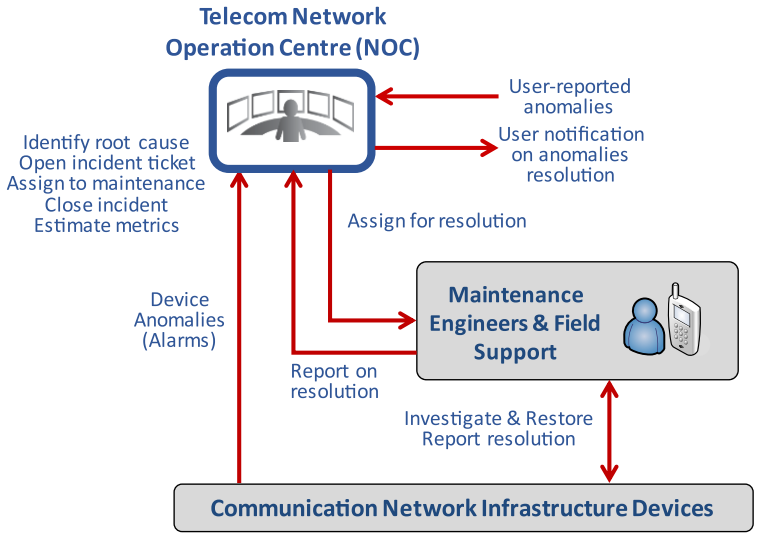


Figure 22 - Actors of an Incident Management and Problem Resolution process

The fault supervision system displays all received NE alarms (from device or through Northbound interface of dedicated NMS) as well as estimated connection faults over multiple layers of infrastructure and service. The operator may also receive service anomalies detected by service users and may manually set a device or a connection as unavailable. This is generally the entry point into the Incident Management and Problem Resolution process. Incident tickets are generally opened in a centralized manner by the network operator upon a preliminary Root Cause Analysis (RCA) across functional layers. The same process determines the potentially impacted services (Service Impact Analysis) through automated propagation algorithm based on dependency relationships.

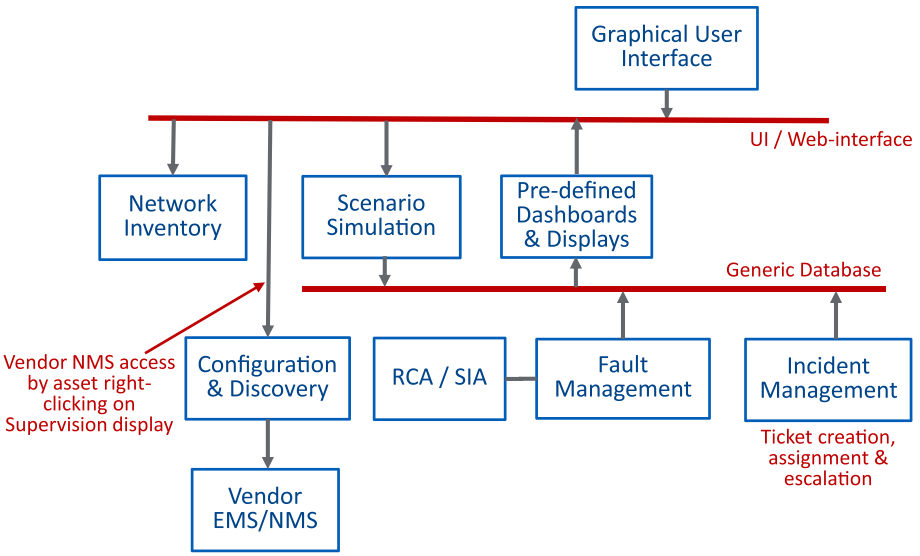


Figure 23 – Incident management and problem resolution functional architecture

1. Upon reception of one or multiple network alarms, the Network operator seeks to identify probable Root Cause using network location of alarms and inter-layer dependencies (digging down) and to identify Impacted Services (moving up in layers)
2. Incident can also be reported by Service User through User/Provider interface (Service desk implemented as Users' Messaging service) or by anomalous performance. Reported service anomalies can be entered into the system by the network operator.
3. Operator creates an incident ticket and assigns it to adequate maintenance staff.
4. Service Manager is informed of any Service Impacts – can be performed automatically using specific Notification Rules
5. Maintenance staff investigate the incident through Sentinel Inventory (device types, shelves, configurations, etc.) and then through Sentinel's Remote Access to Vendor tools (EMS/NMS, Craft, Device HMI), make modifications remotely or on site, and complete the Ticket's report zone. Maintenance staff may run offline Scenario Simulations using Sentinel's Inventory.
6. Operator closes incident ticket. Statistics on outage duration and time to resolve are used for building specific Resolution Dashboard

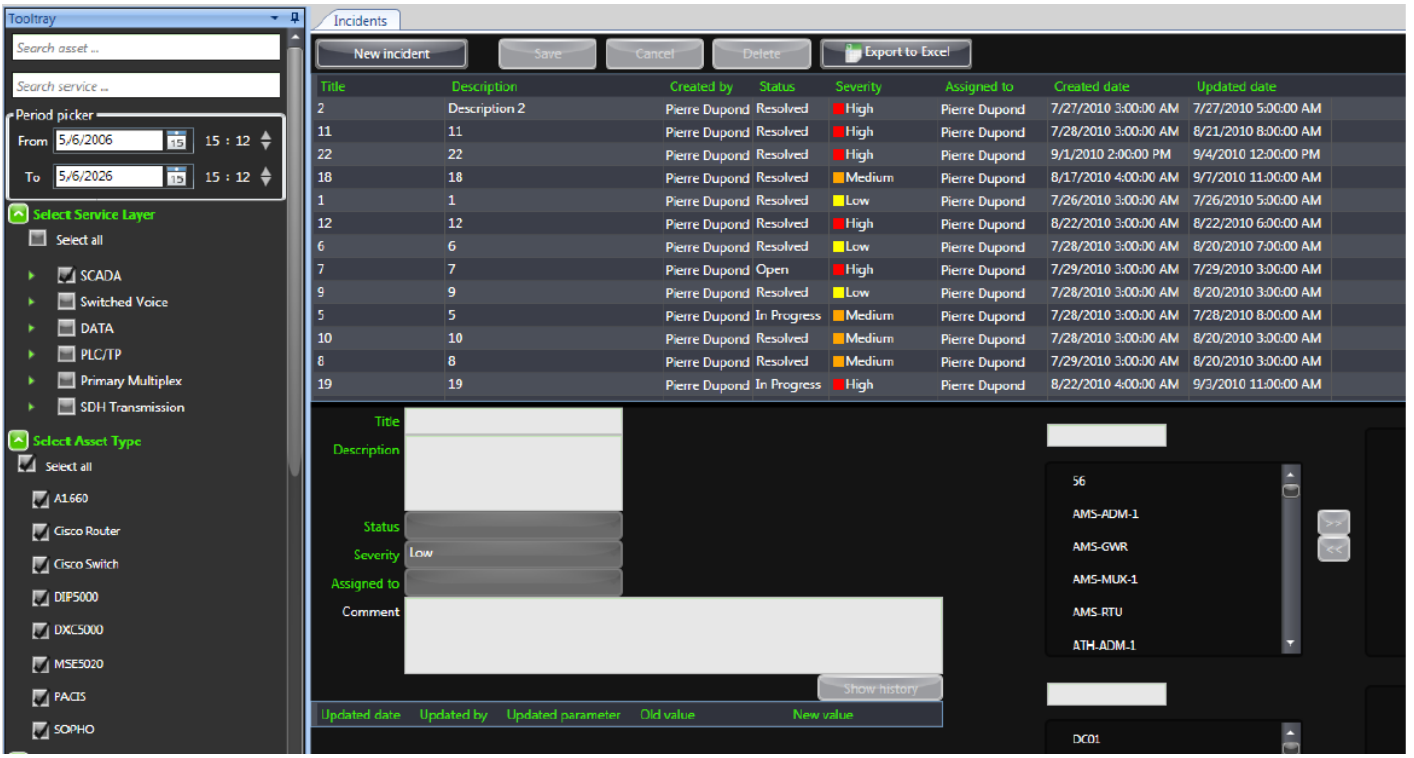


Figure 24 - Sentinel Incident Management user interface (ticketing, assignment and reporting)

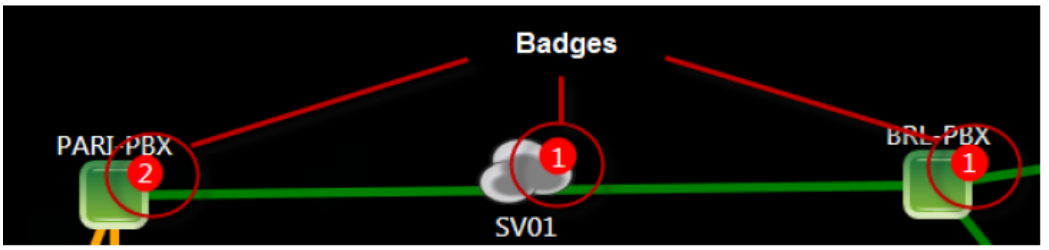


Figure 25 - Incident badges visible on Sentinel Supervision display

Updated date	Updated by	Updated parameter	Old value	New value
11/1/2013 9:38:32 AM	Michael Smith	Status	Open	In Progress
11/1/2013 9:38:32 AM	Michael Smith	AssignedTo	Michael Smith	Michael Smith
11/1/2013 9:38:51 AM	Michael Smith	Status	In Progress	Resolved
11/1/2013 9:38:51 AM	Michael Smith	AssignedTo	Michael Smith	Joe Doe
11/1/2013 9:40:08 AM	Joe Doe	Status	Resolved	Closed
11/1/2013 9:40:08 AM	Joe Doe	AssignedTo	Joe Doe	Joe Doe
11/1/2013 9:40:29 AM	Joe Doe	Status	Closed	Open
11/1/2013 9:40:29 AM	Joe Doe	Severity	Low	High
11/1/2013 9:40:29 AM	Joe Doe	AssignedTo	Joe Doe	Michael Smith
11/1/2013 9:40:29 AM	Joe Doe	Assets	AMS-ADM-1	ATH-ADM-1, AMS-ADM-1
11/1/2013 9:41:44 AM	Michael Smith	Status	Open	Closed
11/1/2013 9:41:44 AM	Michael Smith	AssignedTo	Michael Smith	Michael Smith

Figure 26 - Sentinel Incident Management - Escalation history

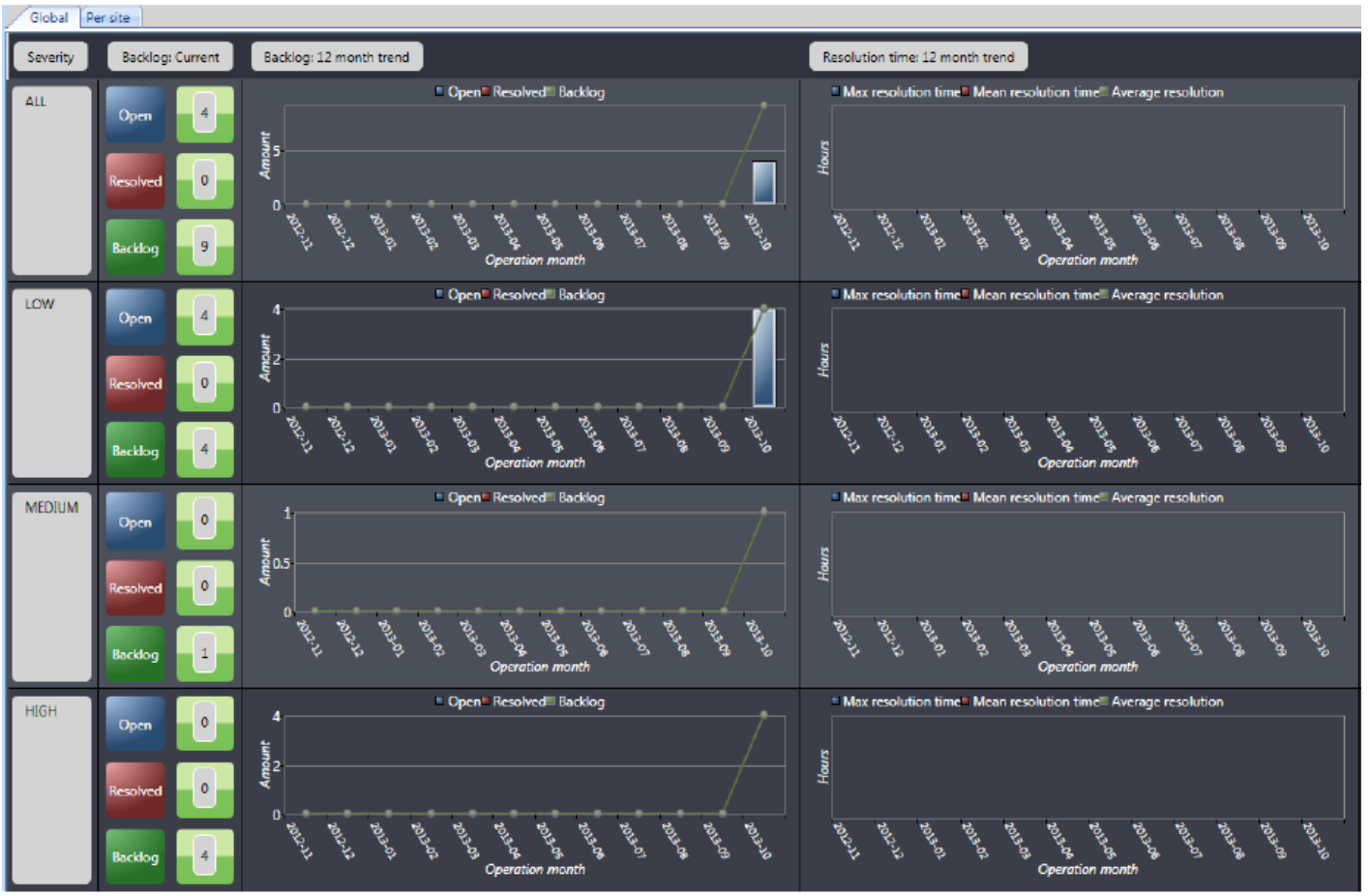


Figure 27 – Sentinel Incident Resolution Dashboard (Open, Resolved, Backlog) with Severity levels and Min/Max/Average Resolution times plotted over a year

7. NETWORK PERFORMANCE AND SERVICE QUALITY MANAGEMENT

7.1. PERFORMANCE MONITORING – "WHY", "WHAT" AND "HOW"?

Contrasting with Fault and Incident Management processes which have been implemented in some form since the early days, Performance and Service Quality Management are relatively new concepts in the Operational Communication Network. For many years, the operational telecom network has been based on permanent connections with constant performance (TDM networks). Proper operation is assured here by anomaly detection mechanisms (Threshold Crossing Alerts) incorporated into devices and covered by Fault Management. The integration of packet-switched communication transforms this situation (as described in section 2.5 above) and renders necessary the monitoring of some performance metrics. Consequently, **the major use cases of Performance Monitoring remain the packet-switched network.**

Network Performance monitoring consists in continuously examining the **capability of the network** to deliver communication services and the evolution of this capability over time. Performance monitoring information is therefore addressed to the Network Operation Center.

"Service Quality Monitoring" on the other hand, is the monitoring of agreed end-to-end metrics defined by Service Level Agreements (SLA), which are perceivable by the service user at User Access Points. Service Quality monitoring checks the **adequacy of the delivered service** for the user's application and its conformity to user requirements. Service Quality information is addressable to Service Manager and hence the Operational Service User as a proof of conformity, as illustrated in figure 28 below.

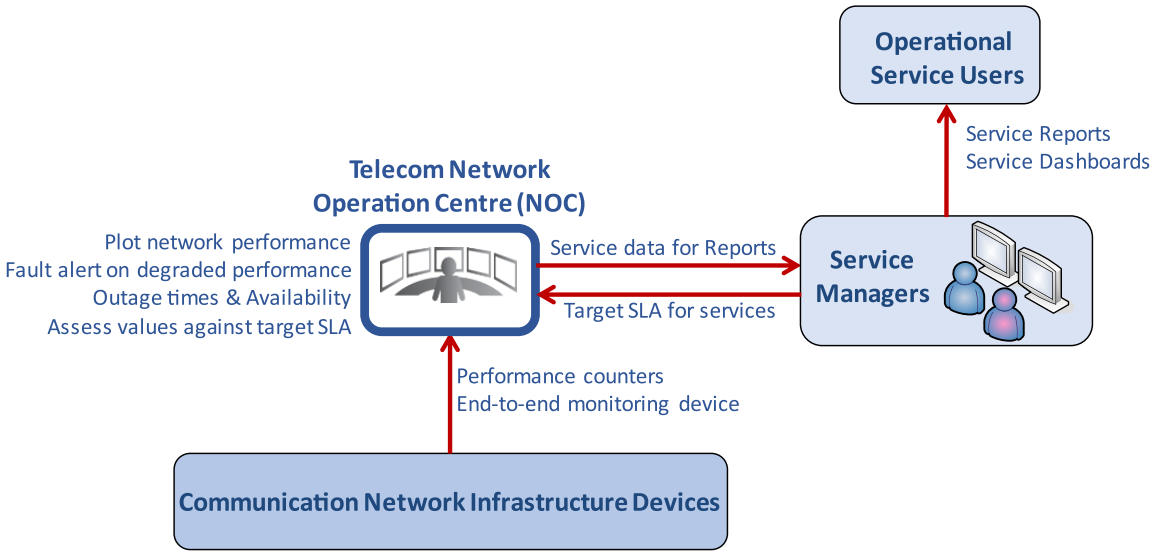


Figure 28 – Actors of a Network Performance and QoS management process

Any varying parameter monitored by the device and stored in its management base (MIB) can be retrieved, processed, and stored in the management platform. For packet-switched networks the most significant parameters are the following:

- Traffic load (TL)
- Packet Delay (PD) and Packet Delay Variation (PDV)
- Packet Loss Ratio (PLR)
- Service Availability (SA)

Performance monitoring can be performed at user initiative, returning one measured value (on-demand monitoring), or in a continuous manner with a preset scanning period.

How and where can data be retrieved?

Performance monitoring consists in retrieving data from the network devices and transforming the data into situational awareness. Data can be retrieved from a network device, or a device manager are presented in figure 29.

The collected data may be used for different purposes as follows:

- Service Availability (SA), and Service Downtime Distribution (DTD) can be estimated using fault monitoring and Service Impact data. SA/DTD are performance indicators generated from Fault Management data. They can further be used for monitoring a contractually agreed level of performance (SLA)
- Threshold Crossings Alerts (TCA) received from the device which collects values and detects a performance anomaly. TCAs are performance-related events fed into the Fault Management process (TCA can also be generated by the platform)
- Data values from the device MIB or from a Device Manager according to pre-set parameters relative to the device, or to a "device port" (e.g. packets/second at a port). Data values may be made available to management system users as off-line Excel files, graphical value evolution trends, statistical metrics (Daily and Monthly Mean and Variance), and Model-based Predictions.
- Model-based prediction uses a statistical model to deliver user-oriented predictive information:
  - What is the maximal value of X for 99,9% of the time?
  - How likely is for parameter X to have a value > (or <) than Xt?
  - What is the domain of X not exceeded for more than 1% of the time?

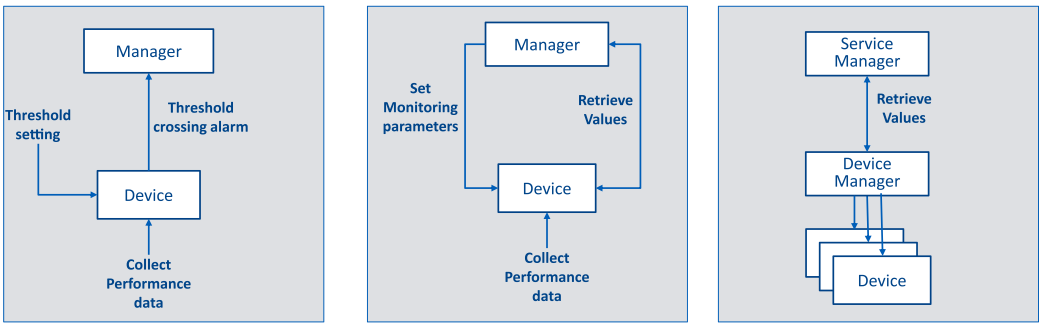


Figure 29 – Value data retrieval for performance management

Sentinel incorporates a group of functions and features relating to the collect, storage, processing, and display of performance data. Performance monitoring in Sentinel concerns availability and down-time of services, value threshold crossings, as well as MIB-stored performance values collected through SNMP. In Sentinel 4.0 data retrieval from Device Managers is performed manually by the operator's remote connection to Device Managers.

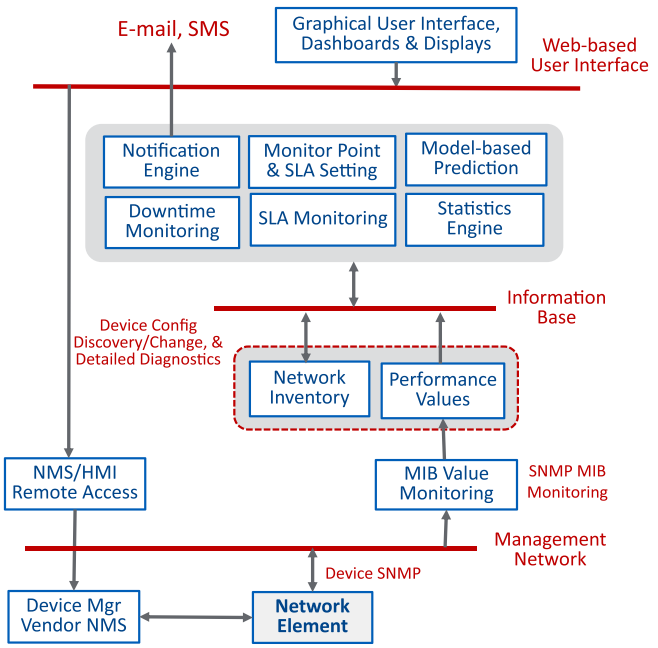


Figure 30 – Sentinel Network Performance and QoS management functional architecture

7.2. SERVICE AVAILABILITY (SA) AND DOWNTIME DISTRIBUTION MONITORING

A point-to-point connection (service) is considered unavailable by Sentinel when both assets at its endpoints are in a state of Alarm. The connection, in this case, goes RED on the supervision display and the system initiates counting “downtime” for the service up to the time that the end assets change status. The duration and the frequency of occurrence of service unavailability are used on a monthly basis to generate outage distribution data on a selective manner (service layers, network zones). Outages are classified as presented below:

Downtime Duration	Monthly Occurrences	Service Outage Category
5 sec – 5 min	5	Short Spurious Faults
5 min – 1 Hour	3	Remotely Resolved Faults
1 Hour – 12 Hours	1	Faults Resolved at Site
>12 Hours	0	Fault Not Resolved at Site

Figure 31a – Monthly service outage distribution

Service downtime is used in conjunction with the total service time for all the selected services to determine Availability (Service uptime/ total service time) on a rolling basis over the last week, last month, and last 6 months. Rolling availability and downtime distribution are presented in User Service dashboard as illustrated in figures 31 (a) and (b).

As it can be observed in the figures, Service Availability is displayed on a logarithmic scale presenting significative boundaries such as 90%, 99%, 99,9% and 99.99%. In contrast with most other availability monitoring systems, here the system shows “Service availability” in line with User requirements rather than “Device Availability” monitored by most other systems and quite irrelevant to the Service User.

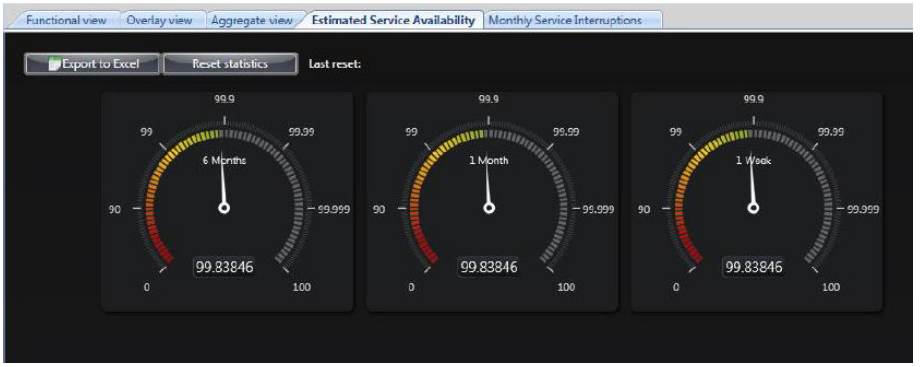


Figure 31b - Service Availability monitoring on a rolling basis

7.3. SERVICE LEVEL AGREEMENT (SLA) MONITORING

Service downtime distribution and statistical availability may be used as criteria for monitoring SLAs (Service Level Agreements). An SLA is a level of performance, agreed upon between service provider and service user, as the minimal quality obligation of the service provider for a given class of delivered services. Sentinel records SLA objectives as rules and targets, with an “alert limit” slightly above the SLA target, allowing to notify the service provider of an imminent miss of a contractual obligation for a user category such as Scada communication.

Type	Name	Service Layer	Subnetwork	SLA target	Alert limit	Intervals/Horizon
Availibility (Percentage)	1	SDH Transmission		70%	80%	1 hour/24 hours
Availibility (Percentage)	2	SDH Transmission		70%	80%	1 day/7 days
Availibility (Percentage)	3	SDH Transmission		70%	80%	1 day/1 month
Availibility (Percentage)	4	SDH Transmission		70%	80%	1 week/6 months
Availibility (Percentage)	5	SDH Transmission		55%	65%	1 month/1 year
Interruption (Count)	6	SDH Transmission		12	10	1 hour/24 hours
Interruption (Count)	7	SDH Transmission		5	4	1 day/7 days
Interruption (Count)	8	SDH Transmission		25	12	1 day/1 month
Interruption (Count)	9	SDH Transmission		68	94	1 week/6 months
Interruption (Count)	10	SDH Transmission		8	5	1 month/1 year
Interruption (Duration)	11	SDH Transmission		6h	4h	1 hour/24 hours

Figure 32 - Setting Availability and Outage time threshold values for SLA Monitoring

SLA targets are set in a specific window as shown in figure 32 and can be based through a Rule concerning the availability percentage, outage duration, or interruption count (occurrence). The results are displayed on an SLA Monitoring dashboard as in figure 33.

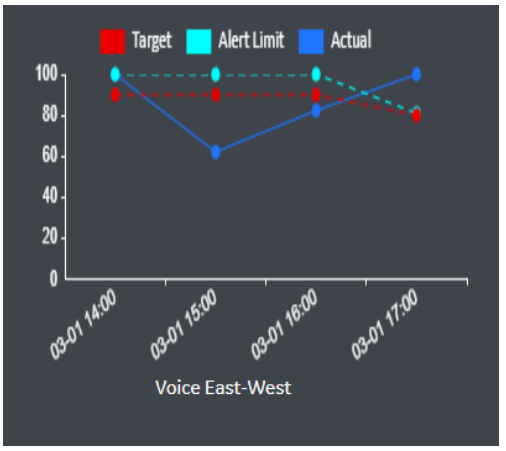


Figure 33 - SLA Monitoring dashboard - Availability, Outage durations and occurrences

7.4. Threshold Crossing Alerts (TCA) on Performance Values

Most devices can generate SNMP Traps on individual performance anomalies (parameters outside nominal range) which will then be treated by Fault Management (Threshold Crossing Alarms are to be set in the device configuration). TCAs are performance-related fault indicators, which can replace bandwidth-consuming value collection both in circuit-based TDM and in packet-switched communication.

7.5. MIB-based Performance Value Monitoring

MIB-stored performance values are polled through SNMP from a given device with a defined periodicity. Parameters that can be retrieved from device MIB for each device type are pre-defined (refer to figure 34) and the location inside the device MIB identified (Object Identifiers OIDs). Monitor Points are registered to specify the periodicity of data collection as well as information on the required processing and storage mode in each case. Value retrieval is performed with a periodicity of every 30-60 minutes selectable at Monitor Point registration. Threshold values can be set for each monitor point in a similar manner. It is noteworthy that MIB value monitoring through SNMP consumes bandwidth across the SNMP management IP network and should therefore be used with moderation to avoid saturating the network and degrading the overall management system performance.

Figure 34 - Retrieval and plotting of device MIB performance measurements and counters.

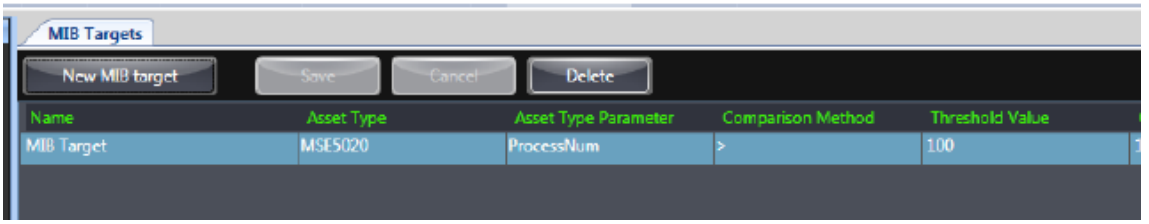


Figure 35 - Setting threshold values to MIB-based Performance parameters (MIB targets)

7.6. RETRIEVED VALUES PROCESSING AND STORAGE – PERSISTENT MONITORING

Performance values can be retrieved on operator's initiative, the system returning one value. They can also be collected in a continuous periodic way in which case they need to be stored (persistent monitoring). Continuously collected values potentially grow to massive amounts of data if captured at many points and over a long period of time. As an example, reading one parameter value every 30 minutes amounts to 17280 values per year. With 100 monitor points across the network, we end up with 1.72 million readings over a year.

At the same time, we can anticipate that individual data values over such a long period do not have much usefulness. We rather need "behavior history". Sentinel maintains a small FIFO stack of 48 real values for each Monitor Point, and it extracts and stores statistical metrics (Mean **μ** and Variance σ^2) for 30 Daily data. Every 24 hours the system calculates and stores statistical metrics from the last day's stored values. Similarly, every 30 days the system calculates and stores monthly statistical metrics from the last 30 daily metrics and stores these monthly metrics in 24 Monthly registers in a rolling basis. In this manner, the user has access to recent data for specific observations, and to the statistical behavior for long term data. Monitor Points can be selected in a filtering zone for being displayed on the persistent value monitoring display as presented in figure 36.

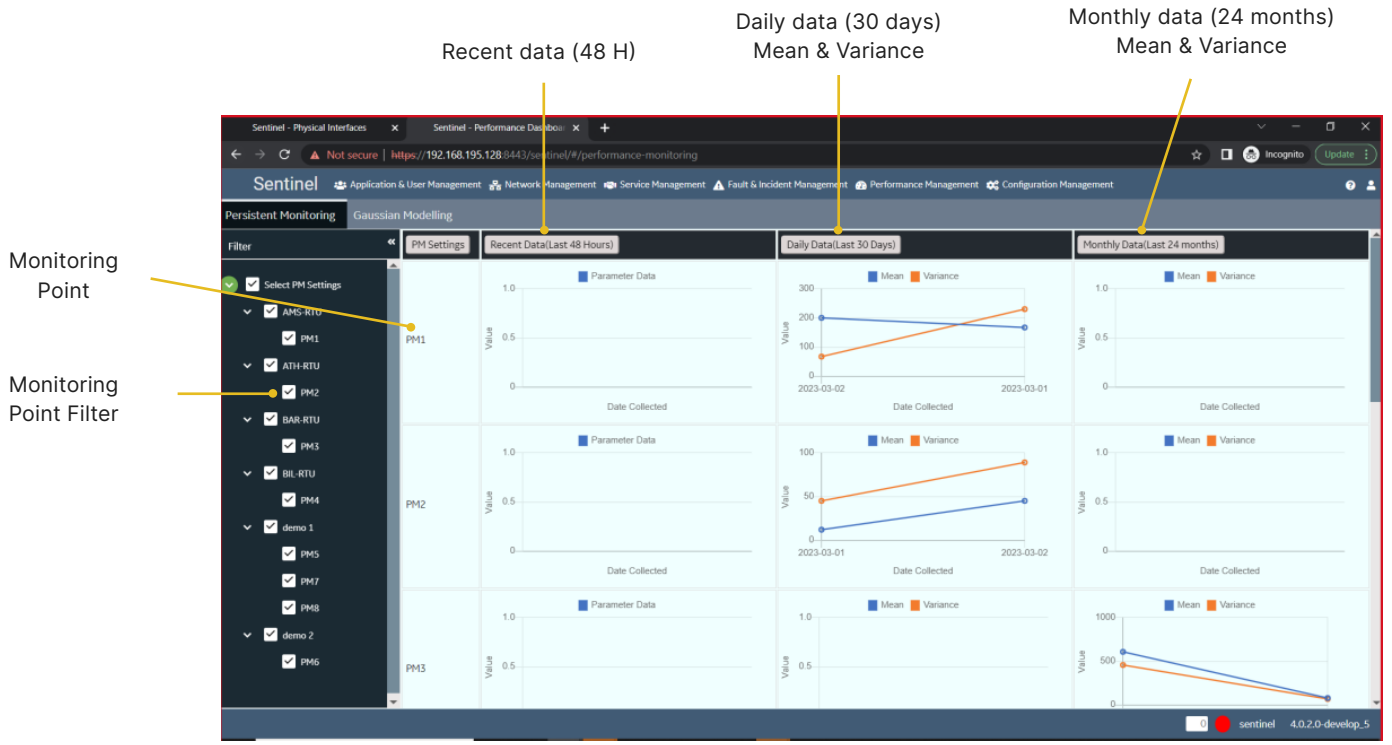
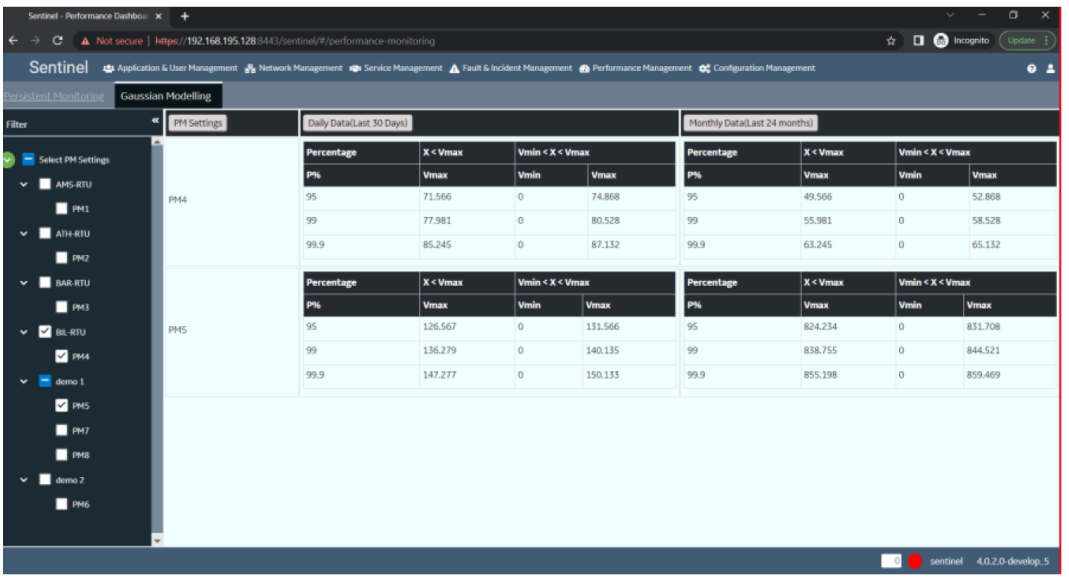
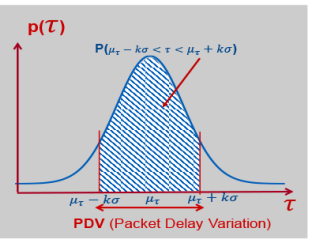


Figure 36 – Sentinel Performance Monitoring

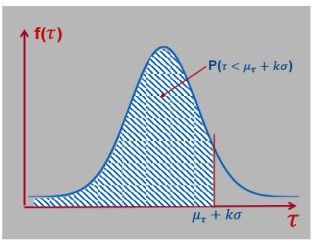
7.7. MODEL-BASED STATISTICAL PREDICTION

The statistical metrics extracted from retrieved data can be fed into a Normal Distribution (Gaussian) model to provide predictive boundary values for a given data set (Monitor Point). This is based on the principle of "percentiles" on a Gaussian distribution curve. In this way, the system returns one-sided and two-sided boundary values for a probability of occurrence of 95%, 99% and 99.9%. This amounts to the value not exceeded by the monitored data with a probability of 95, 99 or 99.9% (one-sided) or a pair of min/max values confining the monitored data with a probability of 95, 99 or 99.9%. Figure 37 presents Sentinel dashboard display for model-based predictions. Appendix B provides the mathematical basis used for this function.





$$Pr(Vmin < V < Vmax)$$



$$Pr(V < Vmax)$$

Figure 37 – Sentinel statistics engine performing predictive estimations. Limit values for 95%, 99%, and 99.9% occurrence probabilities in one-sided (V<Vmax) and two-sided (Vmin<V<Vmax) predictive estimations based on a Normal (Gaussian) Distribution Model

7.8. MONITORING BETWEEN TWO POINTS – NETWORK-LEVEL ETHERNET SERVICE OAM

Service OAM comprises a group of end-to-end monitoring mechanisms defined for Ethernet transport (Carrier Ethernet or MPLS-TP) by exchanging specific supervision messages (OAM-PDUs) between the two "Maintenance End Points" (MEPs) as shown in figure 38. These standard mechanisms allow to check that a virtual connection can be established between the points (IEEE 802.1ag Connectivity Fault Management), and to estimate Time Delay and Packet Loss (ITU G.8013 and Y.1731 for Carrier Ethernet and ITU-T G.8113.1 for MPLS-TP).

Service OAM monitoring is performed at device or specific NMS level once the function is configured. The monitoring results may be accessible at device MIB in which case Sentinel can collect these results as any other MIB-stored performance data and consequently processed and displayed as defined in the previous sections. If performed in the device-specific NMS, the operator can access the data through remote connection to the appropriate NMS as for discovery, diagnostic and configuration actions. In this case, the retrieved values cannot be stored and processed by Sentinel.

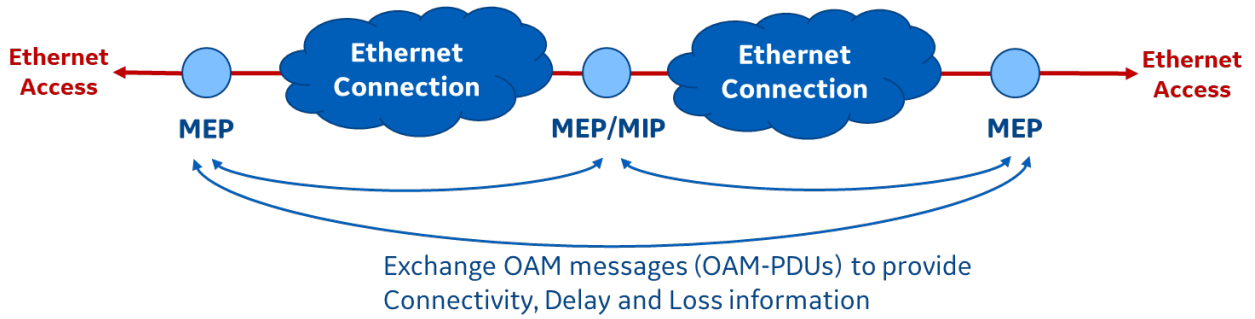


Figure 38 – Service OAM monitoring (MEP/MIP: Maintenance End/Intermediate Point)

8. CONFIGURATION, PROVISIONING & CHANGE WORKFLOW

8.1. SERVICE FULFILLMENT AND WORKFLOW PROCESS

Network transformation planning and engineering undertake network modifications in response to new service requirements and resource usage. These changes may be initiated by the service users (changes in service requirements), by asset replacements, or by detecting recurrent performance anomalies through the supervision of the network.

"Service Fulfilment" concerns all actions related to addition, modification and deletion of services necessitating provisioning or modification of connections and device configuration changes. Network/device configuration change is to be performed through dedicated NMS tools or by direct access to device HMI – Sentinel may be used as a framework for accessing the NMS or HMI. However, configuration change also **requires keeping track of change orders and updating service and infrastructure inventories (change management)** without which a network will rapidly go out of control. Sentinel greatly simplifies this essential process.

As presented in section 2.1 figure 2, Service fulfilment process comprises the following:

- **User Order Handling/Change Handling** – This is the process for an operational user entity (such as the EMS/SCADA dept.) to request the Telecom Service Manager for the creation, modification, or deletion of a service. These operations are handled through non-automated but formalized processes as described under Service User Interfacing and Service Desk below.
- **Service Configuration & Activation** – A service request is treated by the Service Manager using information stored in the Service Inventory (service interface, connection type and capacity, quality parameters, SLA monitoring requirements, etc.). A service request is translated into a network change and resource reservation request by the service manager. When the corresponding network change (circuit provisioning and de-provisioning) is confirmed, then the service inventory and supervision are modified, required service quality monitoring is provisioned and service activation notified to the requesting user. This process is assisted by inventory facilities.
- **Bandwidth & Capacity Provisioning** – Network change requests, described above, must lead to appropriate actions upon the network devices following end-to-end path computation and bandwidth resource reservation performed on Sentinel's Network Inventory system. In this way, the work order for network configuration is prepared, and the inventory/supervision system is modified accordingly. The "network change" work order is executed on network devices using Vendor-specific management systems, device-embedded management applications, or through device HMI. The appropriate manner to change device configuration varies depending upon devices, the complexity of the task and the extent of works. GE Vernova Sentinel provides the Network Inventory as well as a framework for accessing appropriate Vendor NMS and device HMI. For a multi-technology core network, Sentinel network displays can be used to observe segments to build in each sub-network, and then dedicated NMS for provisioning each segment. When the circuit is ready, the service management is notified for activating the service and informing the user as described under Service Configuration and Activation above.

A typical example of service fulfillment process workflow is presented in figure 39 below.

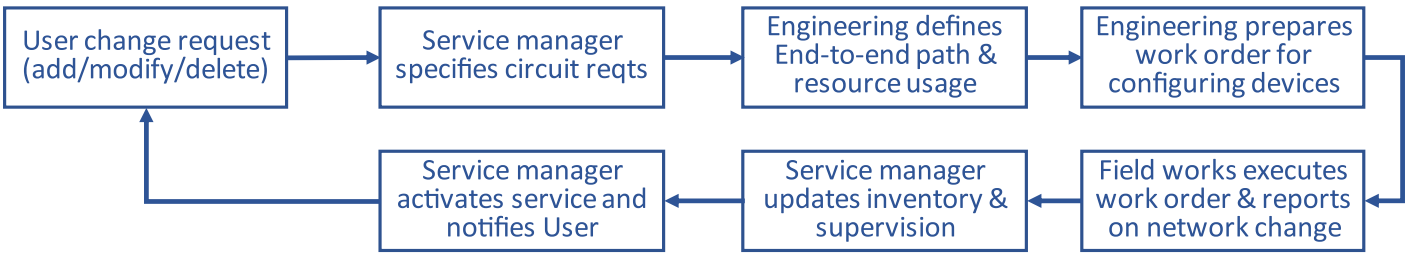


Figure 39 – Service Fulfilment process

As presented in figure 40, three parties interact in this process: Service User requesting change, Communication Service Provider preparing the "digital twin" and the work-order, and Physical Network Implementation team undertaking the works. There is no pre-established automated workflow manager in Sentinel but there are functions and tools to assist every step as shown in figure 40 and described in the following paragraphs.

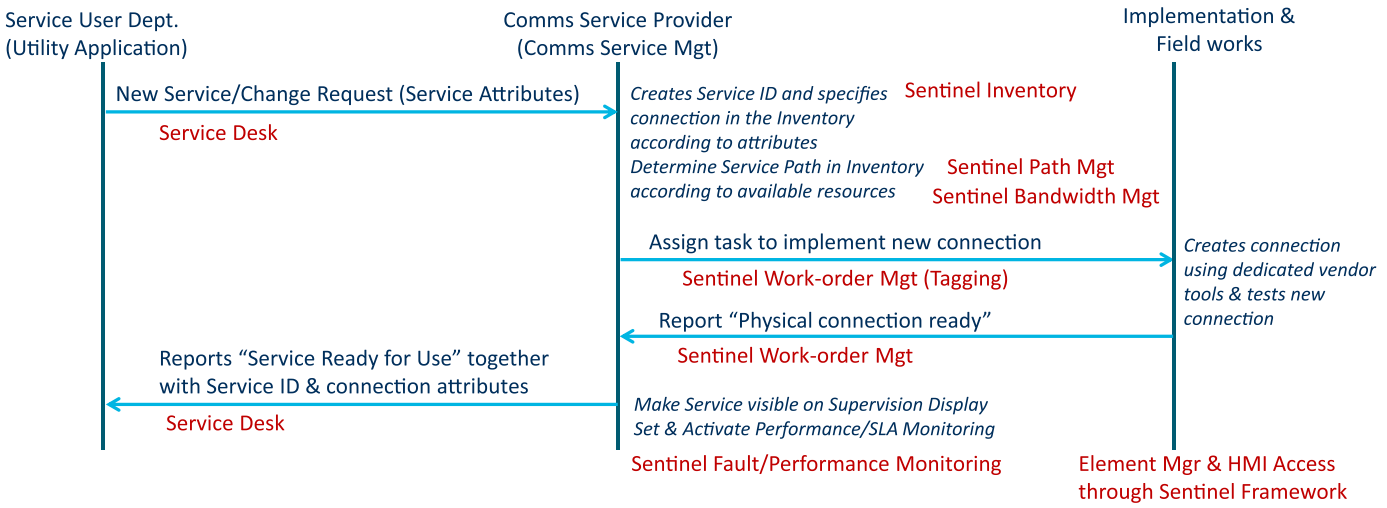


Figure 40 - Service Provisioning & Change Process using Sentinel

8.2. SENTINEL PATH MANAGEMENT AND FAULT SIMULATION FACILITY

Path Finder

At the time of creating a service connection, Sentinel proposes alternate paths for routing the connection across the underlying infrastructure. The user can adopt a path routing or manually replace it by a different path. The adopted path is stored in Sentinel Inventory and can be used for implementation on the physical network.

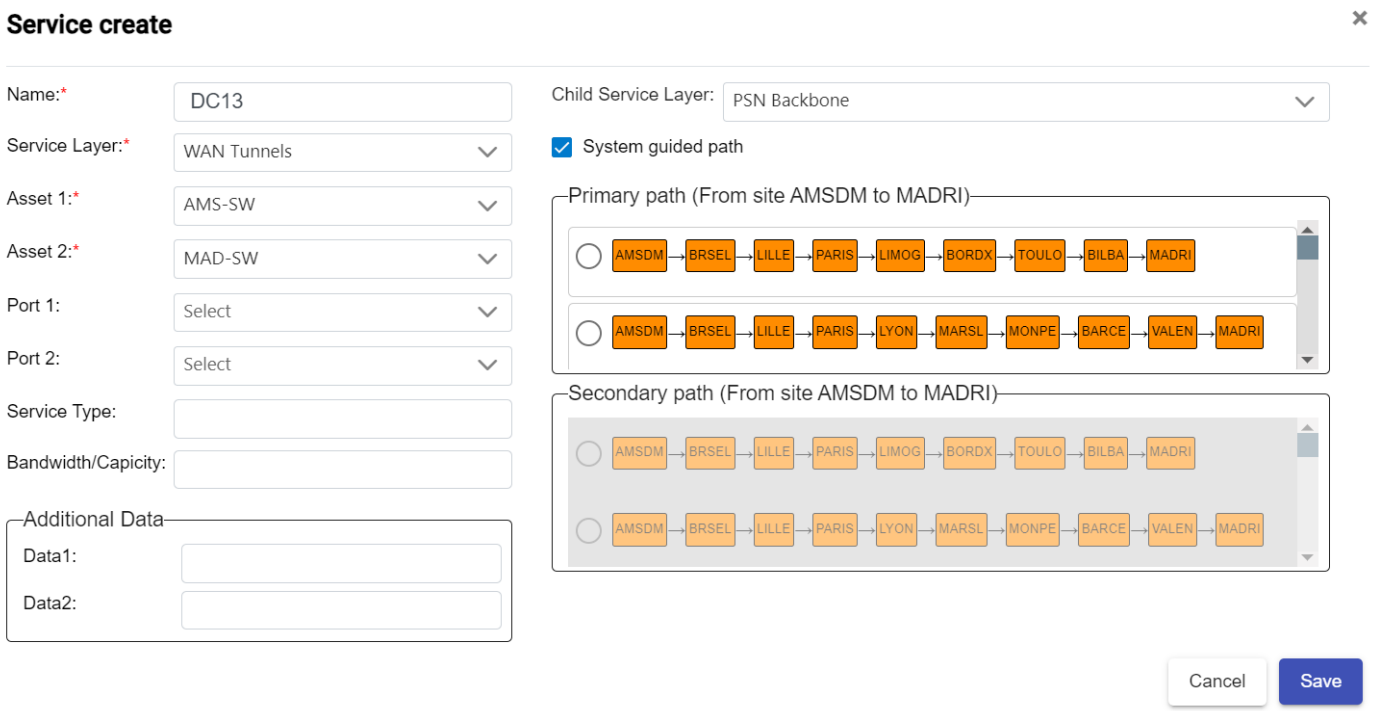


Figure 41 – System guided path finder in Service creation template – Sentinel proposes all possible routing alternatives for the connection Amsterdam Switch to Madrid Switch over the Packet-switched Network (PSN). In this example there are 48 different alternatives for the primary path from which the user shall select one.

Path Tracker

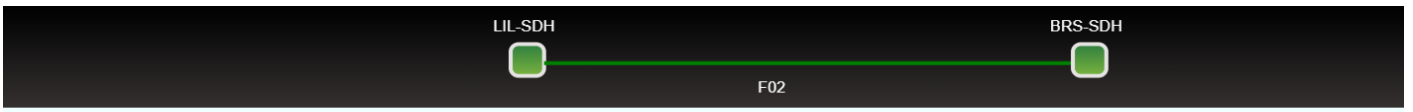
This inventory function allows to select a Service identifier at a given network layer and to retrieve from inventory its path across the network through underlying infrastructure. The Path Tracking operation and display in Sentinel is similar to the Root Cause Analysis function and display presented in section 5.2 and illustrated by figure 18 and 19.

Fault Scenario Simulation

"What-if" Scenarios may be simulated using an off-line copy of the network's path routings and layer dependencies, residing in Sentinel. This inventory-based function allows to check the impact of network fault scenarios or programmed maintenance works on different services. This is particularly useful when provisioning fault resilient paths for services.

8.3. BANDWIDTH MANAGEMENT – PLANNING & RESOURCE OPTIMIZATION

Bandwidth management is another inventory-based function in Sentinel essentially useful for network planning purposes. It allows to determine resource usage according to inventory-stored network information. On selecting a network connection (SDH link F02 in figure 41), the system returns the bandwidth/capacity stored in the network inventory for the connection as well as the bandwidth stored for each of the overlaying services using the selected connection segment in its transport. In the example of figure 41, the SDH connection F02 between Lille and Brussels in under analysis. The link capacity is STM-4 (622Mbps). This link is being used for the transport of 3 Main connections each with a capacity of 2×2Mbps and an Alternate route for a 10×2Mbps PDH link MC03. (Total F02 bandwidth usage: 16×2 Mbps out of 622Mbps).



Bandwidth

Search

Type	Layer	Service Name	Main/Alt	Bandwidth	End Asset A	End Asset B
Analyzed Service	SDH	F02		STM-4	LIL-SDH	BRS-SDH
Client Service	PDH Access	M02	Main	2x2Mbps	BRS-PDH	PARI-PDH
Client Service	PDH Access	M03	Main	2x2Mbps	AMS-PDH	PARI-PDH
Client Service	Voice	SV01	Main	2x2Mbps	PARI-PBX	BRL-PBX
Client Service	PDH Access	MC03	Alt	10x2Mbps	PARI-PDH	BRL-PDH

Figure 41 – Bandwidth Management in Sentinel

9. MANAGEMENT INTERACTIONS – SENTINEL MESSAGING WHITEBOARD

Figure 42 presents message exchange interactions between Operational Service Users and the Service Provider as already shown in figure 3 in the section on Network Management Process. The top diagram concerns service provisioning as described in section 8.1 and the bottom diagram concerns User Perceived Anomaly and Service Impact notifications. In both cases there is requirement for a means of communication between the service user and the service provision organization through the Service Manager.

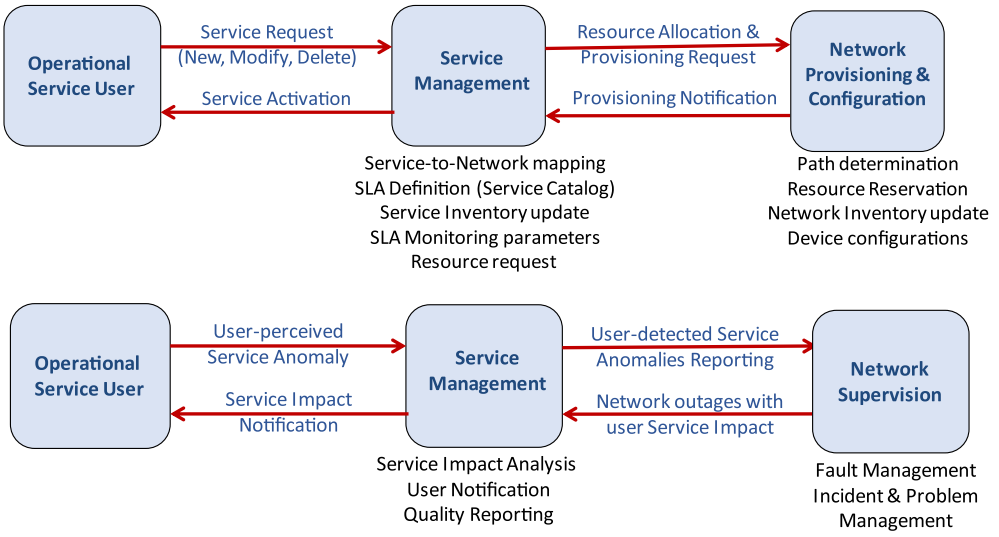


Figure 42 – Operational Service User to Provider communications

Exchanges between Service Users and Service Management are often performed through different means outside the management platform (e.g. e-mail). However, if the User is connected to the Sentinel platform, then Sentinel's "Operations Messaging Whiteboard" may also be employed for fulfilling this requirement. Whiteboard is a closed messaging service between all Sentinel platform users as presented in figure 43. It can be used to assure messaging between different network management actors and stake-holders.

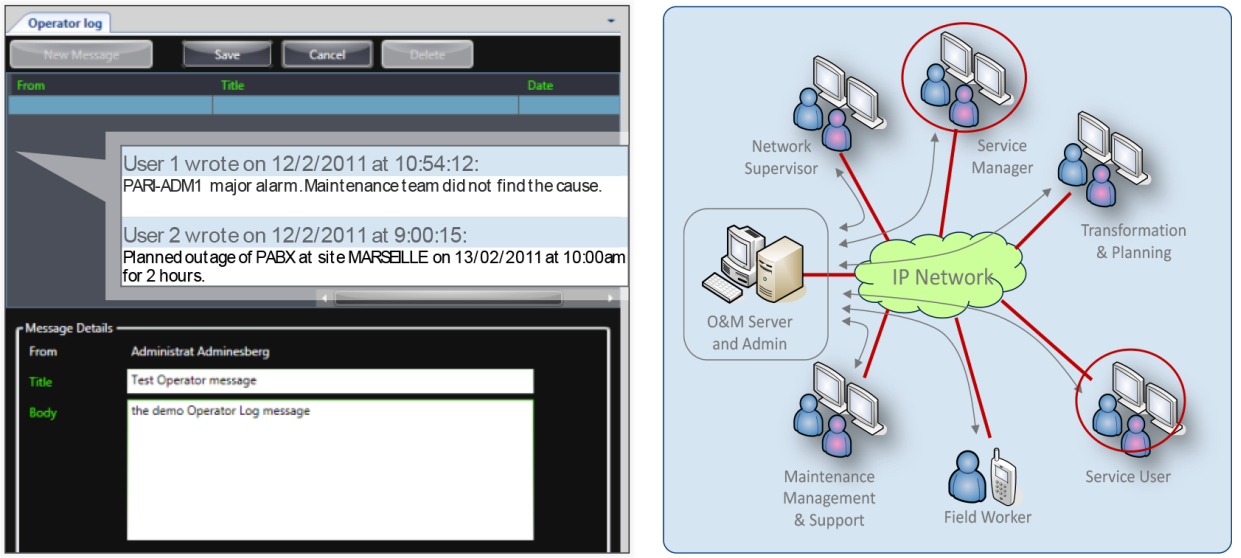


Figure 43 - Sentinel users' communication through Operations Messaging Whiteboard

Other interaction media such as Notification Engine and Incident Management Reporting are already presented in sections 5.4 and 6 above.

10. SUMMING UP

Managing an operational communication network is not limited to a network operation tool but comprise a human organization fulfilling many processes for planning, deploying, operating, transforming, and maintaining the network infrastructure and its available resources, as well as the communication service delivered to the network users. The size and scale of the network and its delivered services determine the complexity of processes to be set up and the extent of formalization and/or process automation that is required. There can therefore be no "one-size for all" approach to the tools and functions.

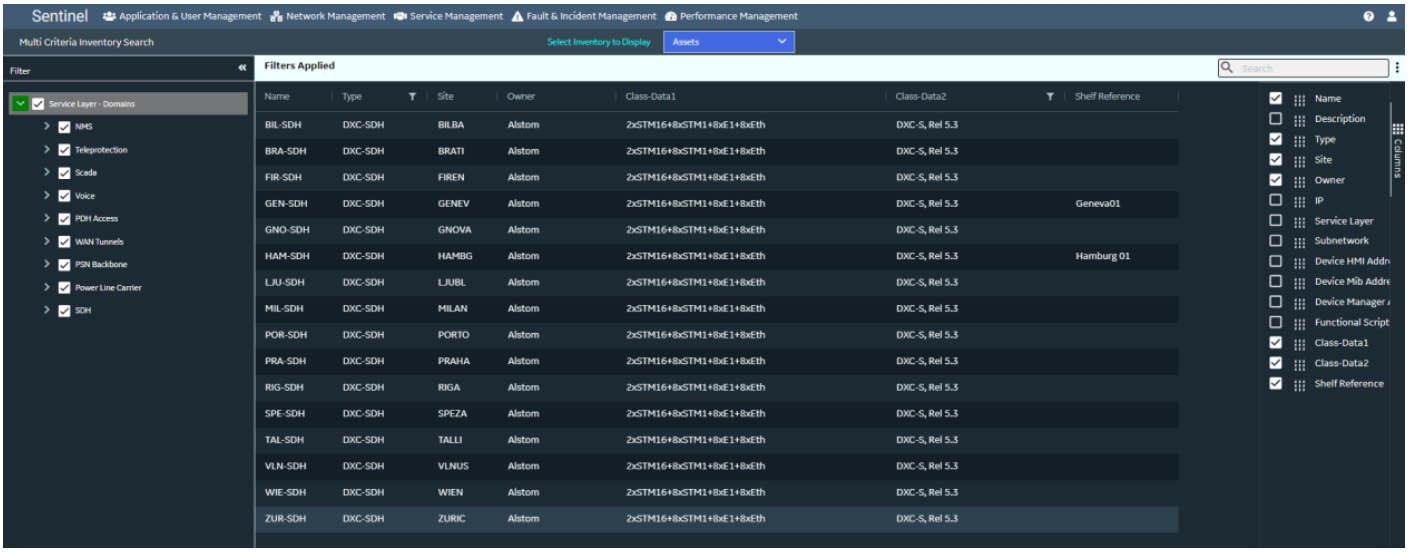
At the same time, operational communications are in perpetual evolution and in most cases constantly growing. It is therefore necessary to adopt a management architecture which can follow this evolution.

Sentinel is a management framework allowing the management platform to grow together with the requirements. From a simple fault and alarm management system to a full-scale Operation Support System, it will accompany the Utility Operational Telecommunications with appropriate supervision information and decisional assistance. Its inventory facilities need not be populated at a same level of detail for all network assets at the same time. It will simply deliver functions according to the level of information which is filled into its data structures.

The common approach in Sentinel principles and user interfaces remains the ease of deployment and of usage, bearing in mind that Utilities need to deliver extremely high quality of service for time-sensitive and mission-critical applications.

The focus is therefore set on operational value with least cost and effort: what is available in dedicated vendor-specific management tools or network devices, is generally not reproduced in Sentinel, but used by Sentinel, allowing the infrastructure to change in time without restarting every time the long and complex integration process.

APPENDIX A – EXAMPLES OF INVENTORY SEARCH AND DEVICE/SERVICE META-DATA

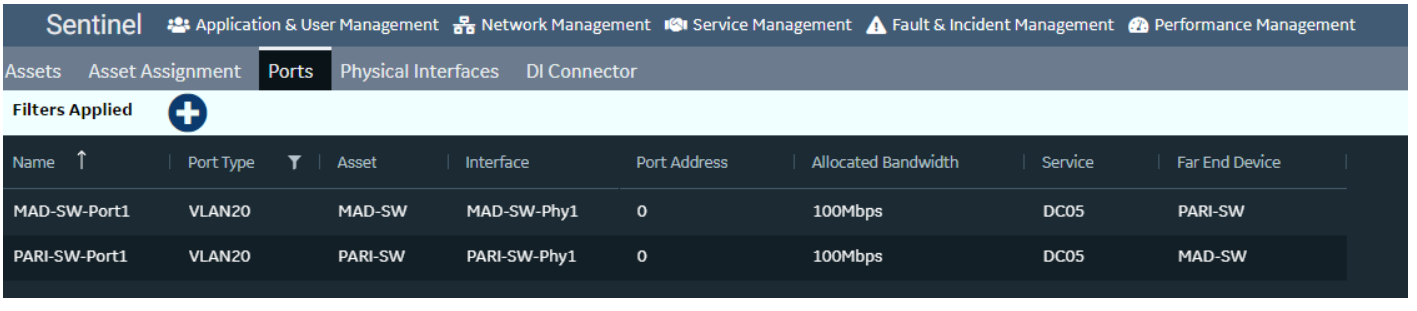


Example 1 – All DXC SDH Devices in the network with Firmware Rel 5.3 in the network

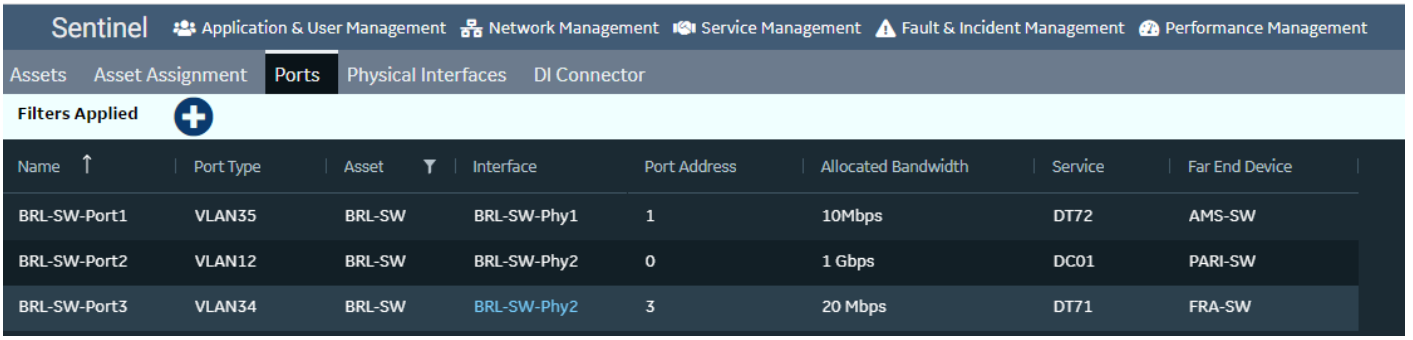
Filters Applied

Name	Type	Site	Owner	Class-Data1	Class-Data2	Shelf Reference
AMS-GbE	DXC-PTN	AMSDM	Project 25	3x10G+8xGbE	eDXC-PTN	Amsterdam 01
AMS-PDH	DXC-Access	AMSDM	Project 25	CHA Rack+2xPS+2xCPU+8RS+4E1+8xIP	eDXC, Rel 2.5	Amsterdam 01
AMS-RTU	RTU600	AMSDM	National Electricity			Amsterdam 02
AMS-SDH	DXC-SDH	AMSDM	Project 25	2xSTM16+8xSTM1+8xE1+8xEth	eDXC, Rel 6.2	Amsterdam 01
AMS-SW	Lynx100	AMSDM	Project 25	DIN rail, dual PS, 8RJ, 2SFP	L110-F2G, 3643-0100, FW Rel2.2	Amsterdam 01

Example 2 – All devices at site Amsterdam and the site's shelf contents



Example 3 – Devices and Service on VLAN20



Example 4 – Ports and Interfaces on BRL-SW Switch

DXC PHYSICAL INTERFACE TYPES (EXAMPLE)

	INTERFACE TYPE	SUPPORTED CAPACITIES	DESCRIPTION	PHYSICAL INTERFACE REFERENCE (CARD TYPE/CARD NO/ INTERFACE NO)
Access	DXC-ACC-12FXO	Analog	Analog Voice - Exchange side	DXC-ACC-12FXO/Y/1-12
	DXC-ACC-12FXS	Analog	Analog Voice - Subscriber side	DXC-ACC-12FXS/Y/1-12
	DXC-ACC-4xC37	subE1	C37.94 Low speed optical interface	DXC-ACC-4xC37/Y/1-4
	DXC-ACC-4xE1	E1	Small format card (mini-slot)	DXC-ACC-4xE1/Y/1-4
	DXC-ACC-8L2L3	L3-IP	IP Router (L3) with 8 LAN interfaces	DXC-ACC-8L2L3/Y/1-8
	DXC-ACC-8xRS	sub64k	Low Speed Data (RS232/RS422)	DXC-ACC-8xRS/Y/1-8
MPLS	DXC-PTN-3×10G	10GE	Card for 3×10GE or 8xGbE	DXC-PTN-3×10G/Y/1-3
	DXC-PTN-8xGE	GbE	Card for 3×10GE or 8xGbE	DXC-PTN-8xGE/Y/1-8
	DXC-PTN-16xE1	E1	E1 Emulation over Packet	DXC-PTN-16xE1/Y/1-16
SDH	DXC-SDH-16xE1	E1	E1 Tributary over SDH	DXC-SDH-16xE1/Y/1-16
	DXC-SDH-STM1-4	STM1, STM4	2xSTM-1 or 1xSTM-4	DXC-SDH-STM1-4/Y/1-2(4)
	DXC-SDH-8xEOS	GbE, ET/FE	Ethernet over SDH	DXC-SDH-8xEOS/Y/1-8
	DXC-SDH-STM16	STM16	1xSTM-16	DXC-SDH-STM16/Y/1

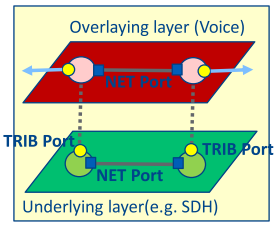
DXC5000 : DXC-ACC
eDXC-PTN : DXC-ACC + DXC-SDH + DXC-PTN

Y : Card Number in the Device

Physical interface types created under Sentinel 4.0 Inventory for GE Vernova DXC devices

SENTINEL 4.0 – PHYSICAL INTERFACE TABLE

NAME	CATEGORY	INTERFACE TYPE	CAPACITY	REFERENCE	ASSET NAME
AMST-SW-Phy1	NET	Lynx-Eth-GE	GbE	Lynx-Eth-GE/1	AMS-SW
AMST-STM-Phy1	NET	DXC-SDH-STM1-4	STM1	DXC-SDH-STM1-4/2/1	AMS-SDH
BRL-SW-Phy1	NET	Lynx-Eth-GE	GbE	Lynx-Eth-GE/4	BRL-SW
FRA-SW-Phy1	NET	Lynx-Eth-GE	GbE	Lynx-Eth-GE/1	FRA-SW
PARI-SW-Phy2	TRIB	Lynx-Eth-ETFE	ET/FE	Lynx-Eth-ETFE/2	PARI-SW
BRL-SW-Phy2	NET	Lynx-Eth-GE	GbE	Lynx-Eth-GE/3	BRL-SW
PARI-SW-Phy1	TRIB	Lynx-Eth-ETFE	ET/FE	Lynx-Eth-ETFE/1	PARI-SW
FIR-SW-Phy1	NET	GES20-Eth-ETFE	ET/FE	GES20-ETFE/1	FIR-SW
FIR-SW-Phy2	NET	GES20-Eth-ETFE	ET/FE	GES20-ETFE/2	FIR-SW
MAD-SW-Phy1	NET	GES20-Eth-ETFE	ET/FE	GES20-ETFE/1	MAD-SW
MAD-SW-Phy2	NET	GES20-Eth-ETFE	ET/FE	GES20-ETFE/2	MAD-SW
VEN-SW-Phy1	NET	Catalyst-Eth-ETFE	ET/FE	Catalyst-Eth-ETFE/1	VEN-SW
VEN-SW-Phy2	NET	Catalyst-Eth-ETFE	ET/FE	Catalyst-Eth-ETFE/2	VEN-SW
LIL-SW-Phy1	NET	Lynx-Eth-GE	GbE		LIL-SW
BRS-SW-Phy1	NET	Lynx-Eth-GE	GbE		BRS-SW
AMST-STM-Phy2	TRIB	DXC-SDH-8xEOS	ET/FE		AMS-SDH



Physical interface table populated for a network under Sentinel. The figure presents the significance of NET/TRIB attribute for each Physical Interface

SENTINEL 4.0 - PORT TABLE

NAME	INTERFACE	ASSET NAME	SERVICE NAME	FAR END DEVICE	BANDWIDTH/ CAPACITY	PORT ADDRESS	PORT TYPE
AMS-SW-Port1	AMST-SW-Phy1	AMS-SW	DT72	BRL-SW	10Mbps	0	VLAN35
BRL-SW-Port1	BRL-SW-Phy1	BRL-SW	DT72	AMS-SW	10Mbps	1	VLAN35
MAD-SW-Port1	MAD-SW-Phy1	MAD-SW	DC05	PARI-SW	100Mbps	0	VLAN20
PARI-SW-Port1	PARI-SW-Phy1	PARI-SW	DC05	MAD-SW	100Mbps	0	VLAN20
MAD-SW-Port2	MAD-SW-Phy2	MAD-SW	DT31	BIL-SW	10Mbps	1	VLAN25
LIL-SW-Port1	LIL-SW-Phy1	LIL-SW	DT01	PARI-SW	50 Mbps	1	VLAN 30
PARI-SW-Port3	PARI-SW-Phy2	PARI-SW	DT01	LIL-SW	50 Mbps	3	VLAN 30
BRS-SW-Port1	BRS-SW-Phy1	BRS-SW	DT02	PARI-SW	20 Mbps	0	VLAN10
PARI-SW-Port4	PARI-SW-Phy2	PARI-SW	DT02	BRS-SW	20 Mbps	4	VLAN10
FRA-SW-Port1	FRA-SW-Phy1	FRA-SW	DT71	BRL-SW	20 Mbps	0	VLAN34
BRL-SW-Port3	BRL-SW-Phy2	BRL-SW	DT71	FRA-SW	20 Mbps	3	VLAN34
BRL-SW-Port2	BRL-SW-Phy2	BRL-SW	DC01	PARI-SW	1Gbps	0	VLAN12
PARI-SW-Port2	PARI-SW-Phy1	PARI-SW	DC01	BRL-SW	1Gbps	1	VLAN12

Logical Port table populated for a network under Sentinel

APPENDIX B – STATISTICS FUNDAMENTALS FOR PERFORMANCE MONITORING

A significant addition to modern operational network monitoring is continuous collection of network parameter values. Extracting awareness from this massive raw data involves basic and standard statistical data analysis which was previously unused in the power utility's telecom network management process. Consequently, it seems judicious to refresh the reader's memory on some fundamentals used in Sentinel value monitoring and to allow appropriate appreciation and usage of statistical data provided by Sentinel. This appendix deals with these theoretical tools which allow data analysis for a sequence of collected values for a given network parameter.

MEAN μ AND VARIANCE σ^2

A sequence of collected data values can be characterized by its statistical metrics Mean and Variance. These metrics represent the overall behavior of the data set, a central value around which the data is dispersed and the data dispersion, without maintaining the information on exact values at any given data capture.

For a data set $(x_1, x_2, \ldots, x_n)$, the mean and variance are given by:

$$\text{Mean } \mu = \frac{\sum_n x_i}{n} = \boldsymbol{E}(x) \text{ : first order expectation of } x \quad (1)$$

$$\text{Variance } \sigma^2 = \frac{\sum_n (x_i - \mu)^2}{n} = \boldsymbol{E}(x^2) - \boldsymbol{E}^2(x) \quad (2)$$

For calculating σ^2, we need first to calculate the first order expectation $\boldsymbol{E}(x) = \mu$, then the

second order expectation $\boldsymbol{E}(x^2)$ and finally the variance $\text{Var}(x) = \boldsymbol{E}(x^2) - \boldsymbol{E}^2(x) = \sigma^2$.

Moreover, the data set can be partitioned into groups (e.g. daily data), determining metrics for each group (e.g. daily mean and variance), and building further metrics from them (e.g. monthly metrics). Similarly, different traffic streams on a same port can be treated as different data sets, each with its own metrics, and then combined to determine the metrics of the overall traffic stream.

NORMAL GAUSSIAN PROBABILITY DISTRIBUTION N (μ, σ^2)

A data set for which we have determined Mean and Variance can be modelled through a standard Probability Distribution in order to exploit its predictive properties. A typical estimation model is a Normal Gaussian density function $\boldsymbol{N}(\mu, \sigma)$ which can be easily manipulated for characterizing network's behavior. As approximated in figure B1 below, the statistical repartition of data samples in a Gaussian distributed data set can be estimated according to its standard deviation σ *(square root of variance: 68.2% (2×34.1) of samples are confined in the range (μ ± σ), and almost 99.9% of samples are below (μ + 3σ).*

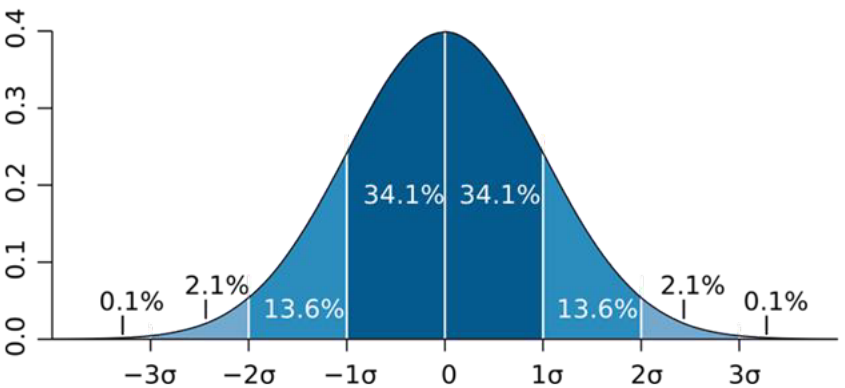


Figure B1 – Data samples probability repartition under a Normal Distribution curve

Source : Wikipedia, By M. W. Toews - Own work, based (in concept) on figure by Jeremy Kemp, on 2005-02-09, CC BY 2.5, https://commons.wikimedia.org/w/index.php?curid=1903871

Hereafter some elements for the understanding of the Normal Probability Distribution:

A Probability Density Function PDF is the probability of occurrence of an incremental value $(x\ , x+\delta x)$. We can therefore determine any probability of occurrence by the surface under the curve (integrate) between appropriate bounds.

$$Pr(X<a)=\int_{-\infty}^{a} f(x).dx \qquad (3)$$

$$\int_{-\infty}^{+\infty} f(x)\ dx=1 \qquad (4)$$

For Normal (or Gaussian) Probability Distribution:

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \qquad (5)$$

Normal Distribution is symmetrical around μ :

$$Pr(\mu-a<X<\mu+a)=2\int_{\mu}^{\mu+a} f(x).dx \qquad (6)$$

Therefore:

$$Pr(\mu-a<X<\mu+a)=2.\frac{1}{\sigma\sqrt{2\pi}}\int_{\mu}^{\mu+a} e^{-\left(\frac{x-\mu}{\sigma\sqrt{2}}\right)^2}.dx$$

Changing the variable from x to t : $\quad t=\frac{x-\mu}{\sigma\sqrt{2}} \quad \rightarrow \quad dt=\frac{dx}{\sigma\sqrt{2}}$

$$Pr(\mu-a<X<\mu+a)=\frac{2}{\sigma\sqrt{2\pi}}\int_{0}^{a/\sigma\sqrt{2}} e^{-t^2}.\sigma\sqrt{2}.dt=\frac{2}{\sqrt{\pi}}\int_{0}^{a/\sigma\sqrt{2}} e^{-t^2}.dt$$

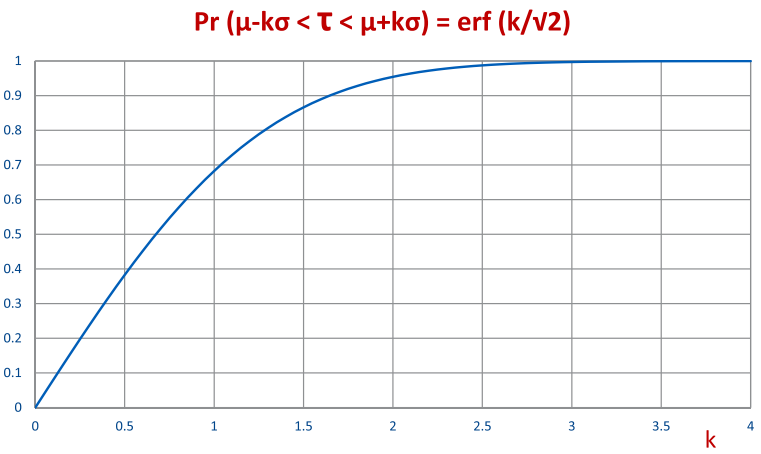
The Error Function Erf(x) is defined as:

$$Erf(x)=\frac{2}{\sqrt{\pi}}\int_{0}^{x} e^{-t^2}.dt \qquad (7)$$

Using $a=k\sigma$, the probability can then be expressed as:

$$Pr(\mu-k\sigma<X<\mu+k\sigma)=Erf\left(\frac{k}{\sqrt{2}}\right) \qquad (8)$$

The probability of values confined in the range $(\mu_\tau-k\sigma,\mu_\tau+k\sigma)$.



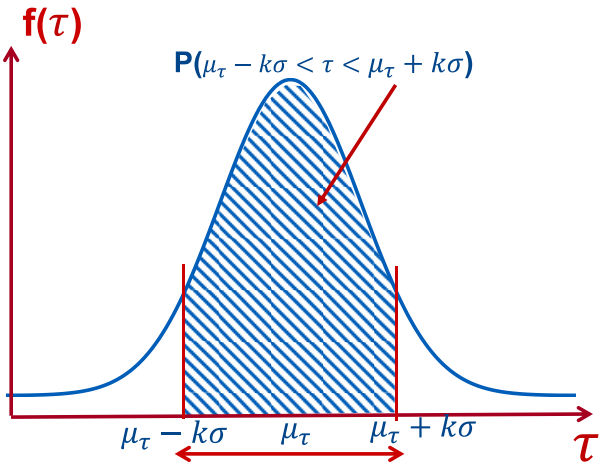
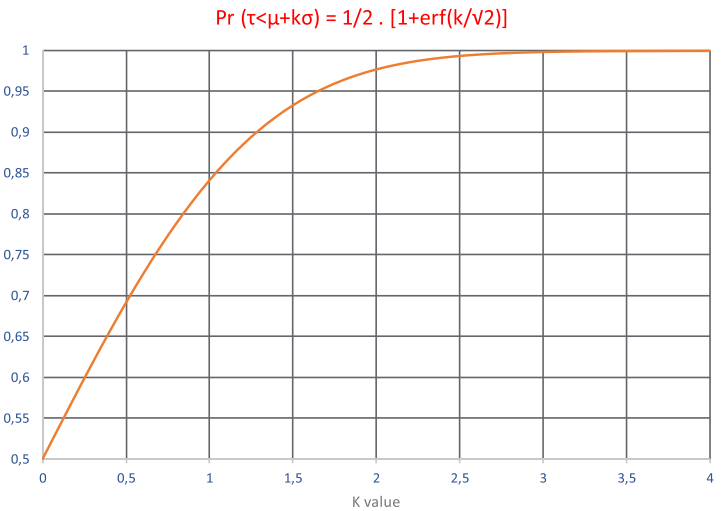


Figure B2 –Probability of values in a specified range around the mean value for $\mathcal{N}(\mu, \sigma)$

PROBABILITY OF τ WITHIN (μ ± kσ)	COEFFICIENT k
0,68 (68%)	1
0,91 (91%)	1,7
0,95 (95%)	2,0
0,99 (99%)	2,6
0,999 (99,9%)	3,3
0,9999 (99,99%)	3,9

To estimate the probability of values being lower than a specified value τ_{max} = μ + *kσ:*

$$\boldsymbol{P}(\tau < \mu + k\sigma) = 1 - \frac{1}{2}\left[1 - erf\left(\frac{k}{\sqrt{2}}\right)\right] = \frac{1}{2}\left[1 + erf\left(\frac{k}{\sqrt{2}}\right)\right] \quad (9)$$



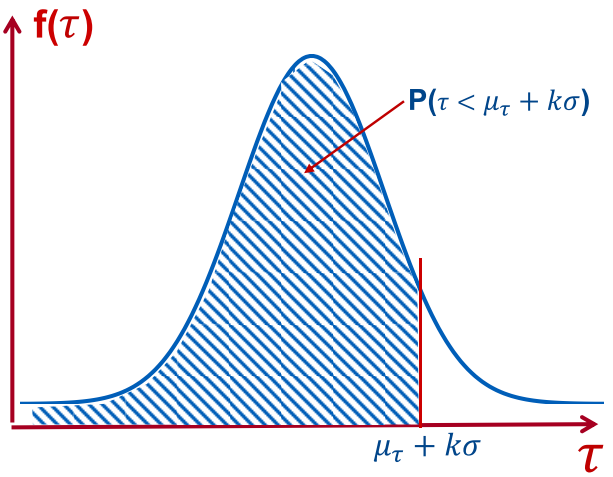


Figure B3 - Probability of values lower than a specified value (μ+kσ) for $\mathcal{N}(\mu, \sigma)$

Some useful values are presented below:

PROBABILITY OF $\mathcal{T} < (\mu \pm k\sigma)$	COEFFICIENT k
0,84 (84%)	1,00
0,90 (90%)	1,30
0,95 (95%)	1,65
0,99 (99%)	2,33
0,999 (99,9%)	3,10
0,9999 (99,99%)	3,72

Spectral Density Model Estimation

Figure B4 presents a sequence of 260 collected data samples with their distribution shown in a histogram. TheMean and Variance of the data set is calculated as (μ, σ). Considering a Normal Distribution model, these metrics are used to plot the Gaussian and to estimate maximum data values for 95, 99 and 99.9% probabilities as shown in the previous section. It is again reminded that these are statistical predictive estimates. They do not give any deterministic "never exceeded" maximal values. The Gaussian curve is a model approximation for the sample data histogram to its left in the figure. The estimations are for the model and not for the real data. The histogram will be constantly changing from one collect to another.

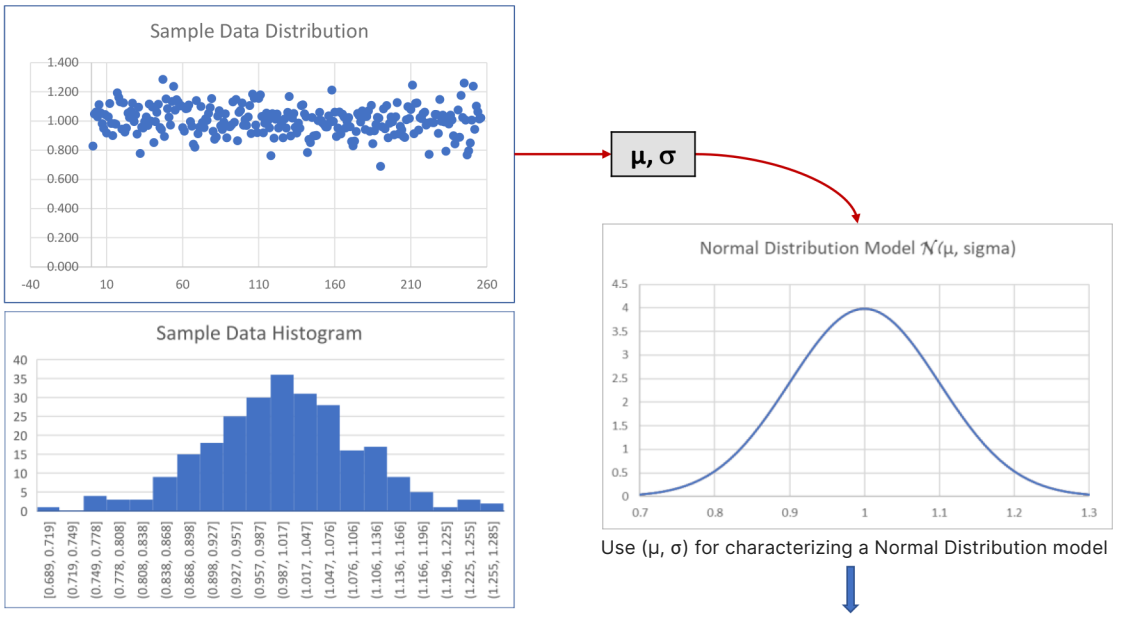


Figure B4 - Density model estimation uses the mean and variance of the captured data to model a Probability Density Function and to estimate data behavior through the model.

The great advantage of the Gaussian model $N((\mu, \sigma)$is the simple usage of the Gaussian Error Function erf (x) to determine the probabilities of T remaining within $\mu \pm k\sigma$ as described in the previous section formula 8.

$$\boldsymbol{P}(\mu - k\sigma < \tau < \mu + k\sigma) = erf\left(\frac{k}{\sqrt{2}}\right)$$

This result is then used to determine one sided probability, maximal variation $(\tau_{max}-\tau_{min})$ useful for delay variation for example, and truncated probabilities as described in the following section. Sentinel predictive estimation uses (μ, σ) calculated from captured data together with the following k-values (derived in the previous section):

(μ, σ)	2-SIDED BOUNDS $(\tau_{min,}\tau_{max})$	1-SIDED BOUND τ_{max}
	$\mu - k\sigma < \tau < \mu + k\sigma$	$\tau < \mu + k\sigma$
PR = 95%	k = 2.00	k = 1.65
PR = 99%	k = 2.60	k = 2.33
PR = 99.9%	k = 3.30	k = 3.10

APPENDIX C – SENTINEL VALUE ANALYSIS IN A UTILITY TELECOM NETWORK

It is difficult to determine the constitution of an operational telecom network in the Electrical Power Utility context. There is a wide dispersion in their size and scale, diversity of equipment and vendors, operation and maintenance process, service quality objectives, and the service provider's contractual engagement. The present appendix provides an analysis based on a hypothetical case which can be used with proper modifications to assess the cost-effectiveness of a solution such as Sentinel in each specific network context.

NETWORK INFORMATION

We consider here an operation communication network comprising 200 grid solutions under the control of two Control Centers (Main and Backup), as well as 4 Technical Offices in the corporate infrastructure of the Power Utility but requiring access to substation data for Asset Management, Grid Engineering, Planning, and Transformation projects.

The Private Communication infrastructure composed of Optical Fibers, Point-to-point wireless, and Power Line Carriers, is used to deliver communication services for

- Protection communications between substation protection relays,
- SCADA communications between substation RTUs and Control Center platforms,
- Data networking between Control Centers, Technical Offices, and substation data servers,
- Voice and data communications for operation and maintenance workforce
- Video monitoring and access surveillance for some critical sites

The supervision of the telecom network is performed from a Telecom Network Operation Center (NOC) which can be co-located (or not) with one of the two control centers, in addition to two Regional Maintenance Centers in charge of two areas of the network.

This hypothetical network is illustrated in the following figure C-1:

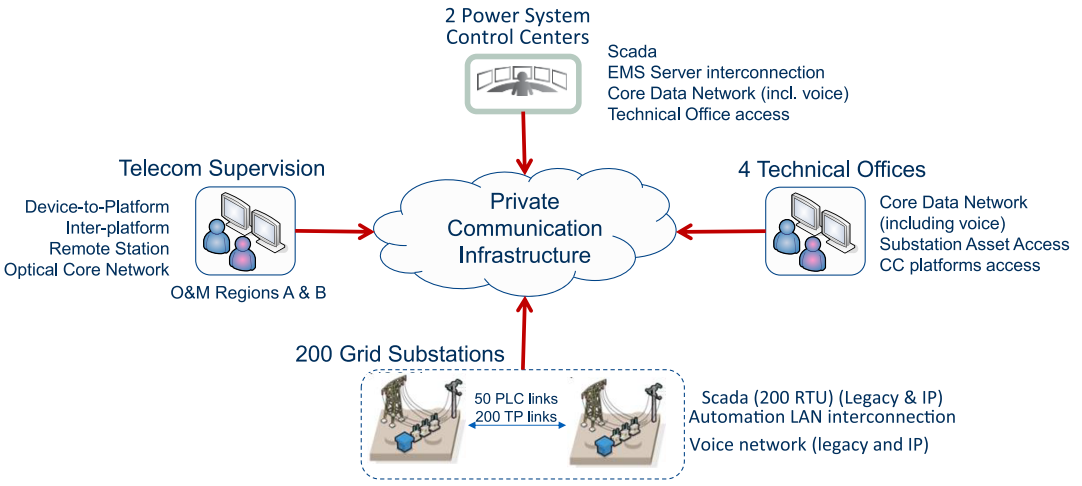


Figure C-1 – Hypothetical power system for Appendix C analysis

The communication facilities of this network of 200 substations are listed in the following table, showing that the listed equipment are associated with 20 Vendor-specific Management platforms.

TYPE OF ASSET	NUMBER OF ASSETS	PROPRIETARY MANAGEMENT PLATFORMS
2000km Optical fibers, 60 Cable Monitoring Points	60	1
SDH / Packet Transport Network Nodes	180	2
Primary Access Multiplexers	100	2
Core Transport Switches (CE/MPLS-TP)	20	1
SCADA RTUs & DSC	200	2
Legacy & IP Telephone Switch (PBX)	30	2
GbE Switches and IP Routers	60	2
Point-to-point Radio Transceivers	5	1
Video cameras in 25 sites	75	1
PLC terminals	100	2
Teleprotection devices	300	2
Auxiliaries, UPS, DC Power Supplies	200	2
Total for 200 substations	1330 Network Elements	20 Management Platforms

It should be noted also that the listed equipment are not un-correlated independent equipment. The functional principles of the network create a great number of network dependencies: a transmission link can operate only if the underlying fiber cable segments are in good health, and the data service between A and B can operate only if all the employed transmission links are in good health, etc. Dependency relations depend on the overlay architecture of the system as illustrated by figure C-2.

Voice network (PBX) and SCADA services are transported over Primary Multiplexers PMUX (sub-E1), or over SDH and MPLS infrastructure (E1, Ethernet), or over an Ethernet/IP network. Video monitoring of substations is transported over an IP network, and Teleprotection services either natively over fiber/PLC or over Primary Multiplexing or over SDH/MPLS.

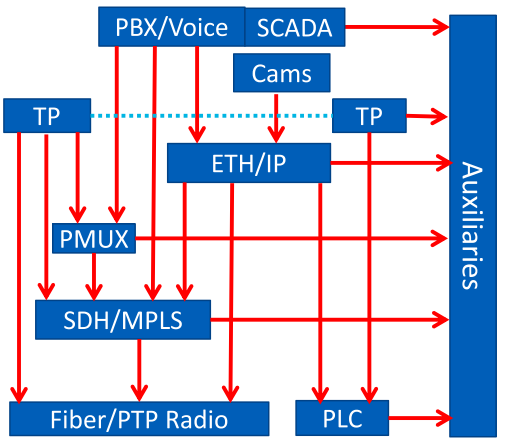


Figure C-2 – Interlayer dependencies in the hypothetical network

In our example, communication services are to be delivered to four distinct Utility customers requiring service reporting and notification for each customer and differentiated quality monitoring for each service. This is the principle of a multi-tenant communication network:

- EMS/Scada platform management EMS
- Substation Facility & Field Worker Management SFF (voice & data, site monitoring)
- Grid Protection & Control Engineering management GPC
- Substation Asset Management & Maintenance dept. AMM

Some possible communication connection service requirements are listed in the following table. These are used to build the Service Catalog and corresponding Service Level Agreements (SLAs):

	SERVICE ID	SERVICE OWNER	DUPLICATE LINK	POWER AUTONOMY DURING OUTAGE	ROUTING RESILIENT/ STATIC	MAXIMAL TIME DELAY	SERVICE AVAILABILITY	SWITCH-OVER & RESTORE TIME	COST OF SERVICE OUTAGE
Protection Relay Comms	PR	GPC	Y	12H	Static	5ms	99.99%	50ms*, 4H**	+++
Scada RTU Comms	SC	EMS	Y	12H	Static	20ms	99.9%	1 sec, 8H	++
Inter-Control Center Links	IC	EMS	N	24H	Resilient	50ms	99.99%	20 sec, 8H	++
Voice & Tech office	VT	SFF	N	8H	Resilient	150ms	99.9%	1 min, 8H	++
Video Monitoring Comms	VM	SFF	N	8H	Resilient	NC***	99%	1 min, 12H	+
Asset Monitoring Comms	AM	AMM	N	8H	Resilient	NC***	99%	1 min, 12H	+
Remote Access	RA	AMM	N	8H	Resilient	NC***	99%	1 min, 12H	+

** Automatic Switch-over, ** Manual Restore, ***Not Controlled*

MANAGEMENT PROCESS ANALYSIS

Based on the network scaling information described above, let us now analyze the tasks to be performed for managing the network and its transported communication services.

First let us consider managing this network through the 20 vendor-specific proprietary NMS as presented in figure C-3 and then using Sentinel

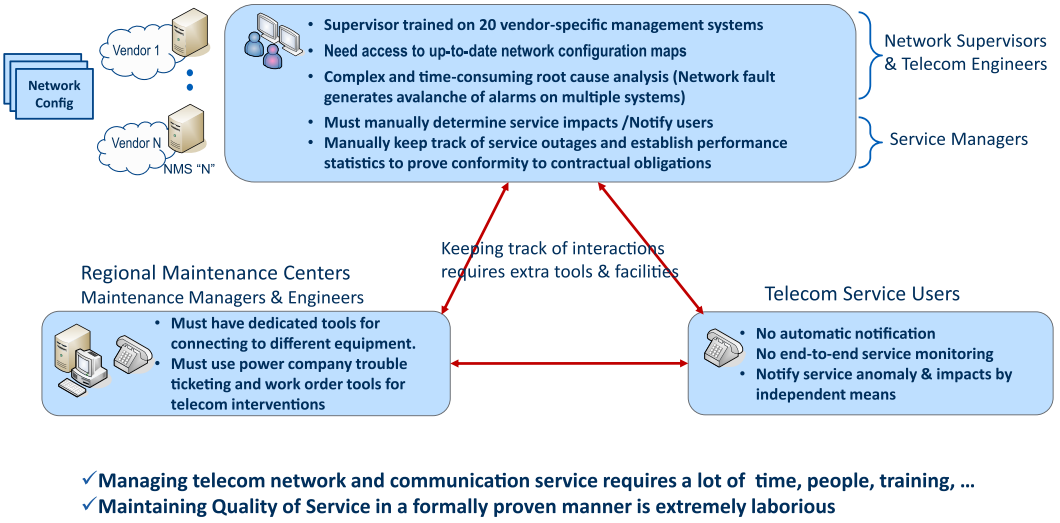


Figure C-3 – Managing the network through Vendor-specific proprietary NMS platforms.

- Network supervisors must be trained to manipulate 20 NMS systems each with specific HMI. Network configuration maps are dispersed with no unique vision of network assets and connections. Determining the root cause of network faults is complex and time-consuming. Similarly, determining the service impact of faults, notification of impacted users, and keeping track of service outages shall require extra time and tools.
- Incident management shall be performed through power company's trouble ticketing and work order tools which are totally disjoint from the network supervision system requiring laborious incident description for assigned maintenance team and for incident resolution reporting. Extra tools are required for allowing management interactions between different actors.

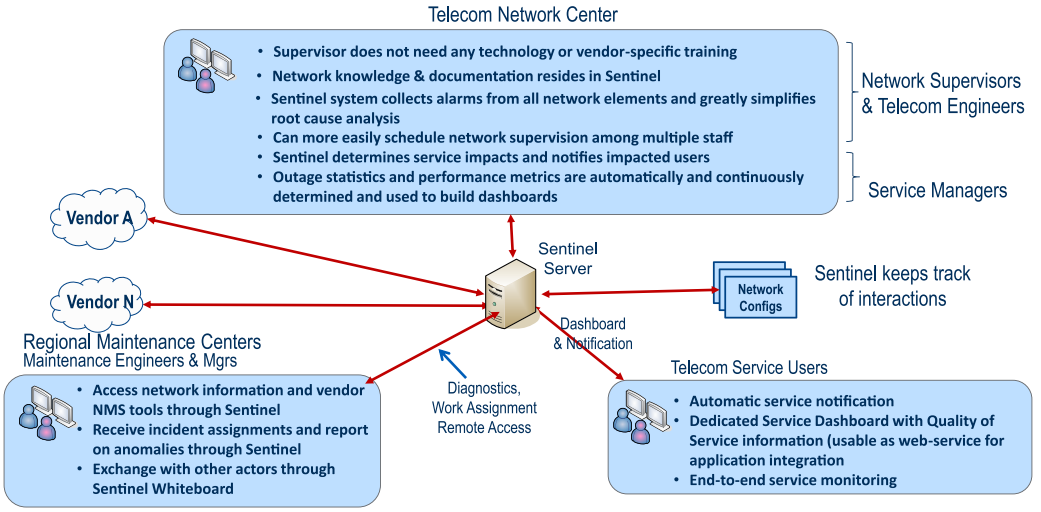


Figure C-4 – Managing the network through GE Vernova Sentinel integrated platform.

Figure C-4 presents the management process in the same context using GE Vernova Sentinel platform.

- Network supervision no longer requires individual systems training,
- Network maps and asset data are integrated through Sentinel's inventory facilities.
- Root Cause/Service impact analysis, user notification, and service outage statistics are automated.
- Incident management is integrated with supervision and embedded network inventory, assigning incident resolution with all necessary data. Similarly, resolution reporting is also integrated into the same system, hence simplifying and accelerating all interactions in the process.

The two management situations of figures C-3 and C-4 are compared in terms of management workload in the following table.

- Operation & Maintenance tasks are listed per process roles of Supervision, Maintenance & Support, Service Management/User Relation, and Network Transformation Planning.
- The monthly workload in fig C-3 and fig C-4 cases are estimated in man-months: a monthly workload of 1 man-months corresponds to a permanent allocated workforce of 1 person.
- The "Size of Workforce" column presents the number of permanently allocated people (A / B) in each process role with vendor NMS only (A) and with Sentinel (B),
- The "Load Reduction" column presents the estimated load reduction obtained through process automation by adopting Sentinel's functions as presented in the last column "Sentinel improvement."

In this analysis, we get a total required workforce of 12 people for managing the telecom network and services without Sentinel and 7 people with Sentinel. In practice most Utility telecom management organizations are under-sized and over-loaded so that many necessary tasks listed in the table such as Reporting, Trending, User Notification, Quality monitoring, and Service-level management, are not (or are poorly) performed. Reducing the recurrent workload by 42%, as concluded by the table, will enable the team to improve service management, increase proactive operation and anticipation, reduce fault restoration time and network down-time, and provide users a better awareness on the state of services and hence increase user satisfaction.

In addition to the recurrent activities of the management workforce, considered in our analysis, management without Sentinel also requires some non-recurrent expenses which will disappear if Sentinel is implemented. These non-recurrent expenses comprise training actions, tools to acquire and configure, software to develop, and must be considered when benchmarking with Sentinel:

- Training for 20 vendor-specific NMS systems and many equipment types
- Training for the usage of network documentation and configuration
- Data Analysis, Statistics and SLA Mgt. and report generation developments
- Software tools and process for building maintenance management statistics
- Secure information exchange between management actors
- Keeping track of incidents and resolution statistics – process, tools, templates, …

These non-recurrent (but rarely one-time!) expenses often represent tens of man-months of effort and very often become obsolete and abandoned fast due to lack of follow-up in the Utility.

ROLE IN THE PROCESS	O&M TASK	MONTHLY LOAD (MAN-MONTHS) FOR NETWORK OPERATION			LOAD REDUCTION	SENTINEL IMPROVEMENT
		NMS (FIG C-3)	SIZE OF WORK FORCE	SENTINEL (FIG C-4)		
Network Supervision	Fault Detection and Localization	0.5	2.0 / 1.5	0.4	20%	Centralized Fault Management
	Problem analysis through collected alarms and user documentation of the network	1.0		0.7	30%	Visual Overlay Interaction Analysis
	Incident management – open trouble tickets, assign maintenance engineers to the resolution of incidents.	0.5		0.4	20%	Simple Incident Management functions
Maintenance & Support	Investigate on the incident with device-specific tools and resolve anomalies by remote or on-site intervention	2.5	6.0 / 4.0	2.0	20%	Centralized Secure Access to Remote dedicated tools.
	Report on interventions and network changes.	1.0		0.6	40%	Reporting through Sentinel Incident Mgt.
	Compile and prepare Incident Resolution Report for the Service /Maintenance Managers and Network planning	1.5		1.0	30%	Reporting through Sentinel Incident Mgt.
	Prepare Maintenance Management Reports, Trends and Statistics (Maintenance Mgt)	0.5		0.3	40%	Automatic Trending & Backlog Mgt.
	Out-of-scope intervention requests due to erroneous or inaccurate fault and anomaly localization	0.5		0.1	80%	Overlay Interaction Analysis Root Cause Analysis
Service Management & User Relations	Service Desk function	0.5	2.0 / 0.5	0.2	60%	Operator Log (white board)
	Perform Service Impact Analysis of network incidents and Notification of Service Users	0.5		0.2	60%	Service impact and notification facilities
	Monitor Service Outages and SLA Fulfillment Service Quality Reports	0.5		0.1	90%	SLA & user/provider management through Service Dashboards
Network Planning & Transf. Eng.	Collect data on anomalies and performance. Build long term metrics & SLAs	1.0	2.0 / 1.0	0.2	80%	Performance trend analysis function
	Determine, plan, and deploy changes for service improvements. Maintain documentation.	1.0		0.8	20%	Network Fault Simulation and Contingency Analysis
Monthly Total		**12.0**	**12.0/7.0**	**7.0**	**42%**	

Recurrent monthly network management workload and its potential reduction through Sentinel platform

REFERENCES AND RELATED DOCUMENTS

1	CIGRE Green Book Springer 2017	Utility Communication Networks and Services Part 3 – Delivery of Communication Services in the Utility Environment Part 5 – Maintaining Network Operation
2	CIGRE Technical Report TB 588/2014	Operation & Maintenance of Telecom Networks and Associated Information Systems in the Electrical Power Utility
3	GE Vernova Technical Talks	Maintaining critical communication services: From awareness to software control
4	IEEE 802.1ag	Ethernet Connectivity Fault Management (CFM)
5	ITU G.8013/ Y.1731	Operation, Administration and Maintenance (OAM) functions and mechanisms for Ethernet-based networks
6	ITU-T G.8113.1/ Y.1372.1	Operations, Administration and Maintenance mechanisms for MPLS-TP in packet transport networks

For more information, visit
gevernova.com/grid-solutions

GEA-N50682
English
251009

GE VERNOVA