GE VERNOVA

Network-aware Telecom Management with

INTERACTING SUPERVISORY AND INVENTORY SYSTEMS

Whitepaper

Grid Solutions

INTRODUCTION

Facing the rapid digitalization of the electrical power system, utility communications are undergoing extensive transformation requiring new information flow requirements. The transformed communication network, often much larger than the existing one and integrating many more technologies, necessitates versatile and easily accessible network information systems as well as a structured end-to-end network supervision system to enable its planning, deployment and operation. It is particularly useful for the operators to rapidly relate network status data captured on the network with engineering configuration data stored in the information system. Many diagnostics and problem resolution tasks require swiftly moving back and forth between the real-time network status and network/equipment configurations.

GE Vernova's e-terra™ Sentinel Network Management and Smallworld™ Network Inventory software solutions enable the association of status and configuration information. This association is a cornerstone for power utilities operating dedicated telecom networks allowing gradual evolution to a full-scope Operation Support platform integrating and enhancing previously distinct information silos, network management tools and operational processes for:

- Network planning,
- Network deployment and transformation,
- Network fault supervision,
- Service assurance,
- Performance monitoring,
- Maintenance & field worker support,
- Service management - customer dashboards, SLA monitoring and service statistics

MANAGING UTILITY OPERATIONAL NETWORKS

Communication networks that connect grid substations and control platforms and allow the interaction of people, platforms and devices across the power system, are undergoing substantial change. Multiple factors are driving this change with the most significant being as follows:

- Data exchange across the grid is growing explosively due to the multiplication of smart "communication-intensive" applications.
- The network perimeter is growing due to more assets and locations needing to be covered by smart applications, leading to more telecom technologies being adapted to new situations.
- New generations of telecom technology are being deployed while the older ones are still in place for a long time due to the slow migration process.
- New asset maintenance processes are increasingly deployed requiring remote access to devices and platforms, for health monitoring and diagnostics from Utility technical offices and for remote support of field workers in the substations.

A great challenge in this context is how to manage an evolving, multi-technology, and multi-vendor telecom infrastructure to deliver services with guaranteed level of quality for multiple groups of users with different service requirements.

- Evolving and multi-technology telecom infrastructure – technological migration both in the power system and in the telecom network brings changes to service requirements and communication solutions. Managing such a network requires a technology-agnostic approach to network supervision so that network evolution does not lead to the need to replace management systems. Moreover, keeping track of infrastructure and service evolution requires a centralized, structured Network Information System to maintain a unique and coherent set of network information for all management actors (network planning, deployment, transformation, operation, and service management).
- Multi-vendor telecom infrastructure – For many years, operational telecom networks have been managed exclusively through the dedicated supervision and configuration tools procured together with telecom equipment. In practice, most utility networks today have 10 - 20 different vendor-specific network management platforms managing optical devices, wireless systems, access multiplexers, Ethernet switches, etc. Situational awareness, however requires the association of information from different devices. A vendor-agnostic network supervision associating information from different types and layers of infrastructure is therefore required.
- Guaranteed service quality for multiple groups of users – An operational telecom network essentially provides pre-established functional planes connecting peers across the grid:
  - Grid management plane connects substation control units to control centers,
  - Protection & Control plane connects protection relays and control devices, - Facility Management plane connects monitoring devices to a monitoring platform, etc.
- Service management is the capability to deliver relevant service information to users on the quality of the delivered communication services through User Dashboards (availability and outage statistics, latency, throughput, ...) as well as impact notification for service user groups when it is estimated that a network fault may impact some of their services.

MULTI-LAYER NETWORK MANAGEMENT

Figure 1 below presents a typical network and service model applying to many operational communication networks. In this model, one can distinguish multiple layers of technology composing the infrastructure plane, collectively delivering a "virtual infrastructure" across the grid enabling the connection of peers for different user services, represented as "user service planes".

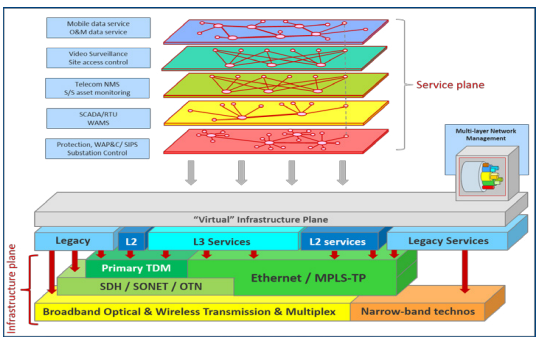

Figure 1 – A typical network model for operational communications in the power utility

Telecom device and platform connectivity for network management is itself one of the applications requiring communication services for delivering alarms, event messages, performance measurements and control information, as well as management workstation to management server connections. This is shown as a service plane, called Telecom NMS, possibly sharing resources with other substation asset management applications (e.g. substation device condition monitoring).

The management platform must establish cause and consequence relationships between events received from different layers of infrastructure to allow fault identification and localization across the multi-layer network (root cause analysis) and consequently to determine service impacts due to network anomalies.

This implies that the platform has access to connectivity information at each layer and on inter-layer dependency relationships. This information may reside in the supervision platform, populated manually by the network operator, or in larger networks, uploaded from a centrally managed Network Inventory.

A GENERIC NETWORK MANAGEMENT ARCHITECTURE

Figure 2 represents a network management architectural model distinguishing the different components and roles in a full-scope management process:

- Network supervision performed from the Network Operation Centre (NOC) allows an operator to be informed of the state of the communication network in terms of faults, performance and configuration changes. This is the basis for a "proactive management" – being informed of network anomalies and taking consequent actions before the network user perceives the anomaly through the quality of the delivered service. Detecting network anomalies requires the reception of network health information from all network devices through events and alarms, and through cyclic measurement of end-to-end performance. It also necessitates a full knowledge of devices, configurations and network interactions generally stored in a network inventory.
- Network maintenance and field support requires an incident management process initiated by Network Supervision described above and a corresponding incident assignment. Maintenance and field intervention also requires access to more detailed analysis tools, often the vendor's dedicated element management tools and platforms, as well as up-to-date network documentation residing in the network inventory. Upon intervention, it is essential to report to the network supervision and to get the network inventory updated.
- Service Management is the part of the management process in contact with the Service Users, notifying the user of any impact of network anomalies, or to notify the supervisor of user-perceived service anomalies for "non-proactive" service restoration. Service management is also in charge of assuring the respect of contractual service obligations (Service Level Agreements) through SLA Monitoring, providing Service Dashboards with main quality metrics such as service availability and outage time distributions.
- Network planning and transformation engineering is the process for deploying new device and transforming the network and must therefore have access to network configuration information and get it modified accordingly, must receive new user requests, and must coordinate outages with the network operation.

This architectural model highlights the fact that a simplified but highly reactive management process requires an integrated information platform to cover real-time event data collection, data sorting and visualization through physical and logical configuration data residing in a network inventory, and process-based exchanges across the network operation organization to allow highly dependable and fast service restoration, as well as operational user relations and smooth network transformations.

There is clearly a need to manage physical and logical inventory in conjunction with the network management platform, Service management and incident management. GE Vernova's e-terra Sentinel Network Management and Smallworld Network Inventory provides this combined management solution.

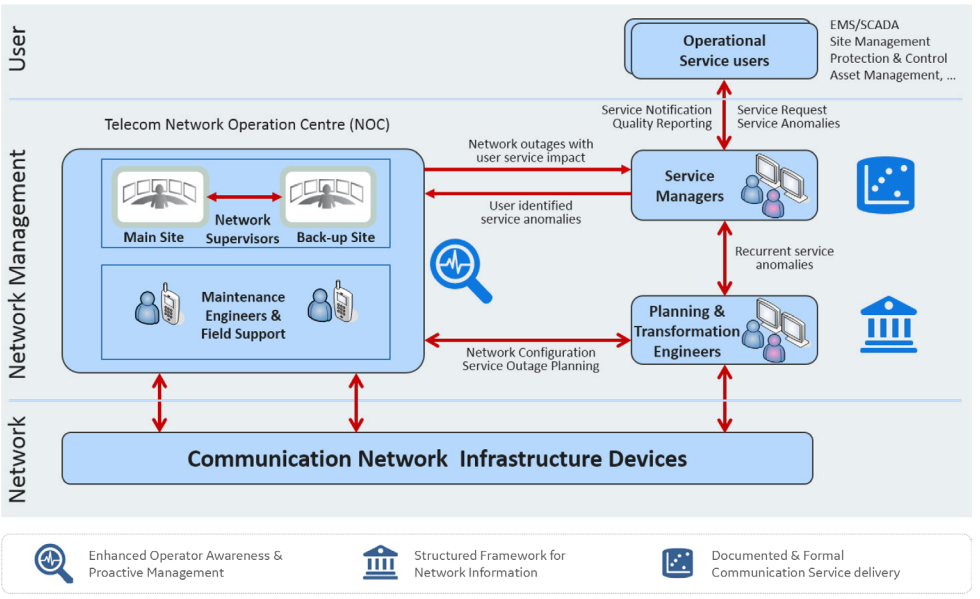

Figure 2 - Full-scope management of utility dedicated telecom network and operational communication services

WHAT IS E-TERRA SENTINEL?

e-terra Sentinel is a vendor-agnostic management platform specifically designed to fulfil the requirements of electrical power utilities' operational communication networks. Particularly, the following features and capabilities distinguish it from other management platforms presently existing on the market:

1. **Multi-vendor and multi-technology** – Sentinel integrates any equipment supporting SNMP (Simple Network Management Protocol) which is the case for the majority of telecommunication and networking equipment today. This assures the flexibility of constructing the network with any building blocks best suited technically and economically without committing for the future to any specific single vendor. However, collecting event information is only a starting point. The value of Sentinel resides mainly in "how to exploit collected data to assure enhanced operator awareness, a more proactive network management, faster service restoration, as well as monitoring user-facing quality of service.

2. **Easy to deploy, maintain and operate** – Sentinel provides a powerful solution for monitoring, supervising and reporting on telecom equipment and services in a perimeter and scale adapted to grid operation networks. It takes into consideration the fact that power utilities cannot allocate extensive resources to their telecom supervision tools and facilities. The "toolbox" is therefore restrained to those tools which are relevant for the "utility operational network". This reduces cost, complexity and underlying platform requirements, as well as the training and comprehension effort for potential users (system maintenance, platform administration, network supervision, service monitoring, etc.).

3. **Fully under Utility control** – Sentinel resides entirely inside the power utility's premises and infrastructures and its normal operation requires no links to external facilities assuring hence the full control of the Utility over its network supervision process and the security of information. The platform can however be connected to other platforms for becoming a constituent of the company's information management architecture.

4. **Service-based principles** – Application connections perceived by the operational network users (e.g. SCADA circuits) do not use necessarily a single technology end-to-end across the connection (e.g. wireless from the RTU to an optical access point and then backhauled through fiber to the center). Moreover, a single technology is not necessarily employed for all connections of the same application (e.g. wireless used for certain RTUs and fiber for others). The service management of Sentinel takes account of these essential principles. This is achieved through partitioning into service layers (e.g. SCADA), functional information transport layers (e.g. Ethernet whatever be the underlying media) and technological layers (e.g. optical SDH) without any distinction of vendors and equipment types at each layer.

5. **Root Cause Analysis and Proactive Service Impact Detection** – Logical dependence relations (parent/child relations) defined between layers give the interaction relations. (The logical link between RTU1 and the center passes through sub-network 1 and a back-up link passes over sub-network 2). These dependencies allow, in the top-down sense, Root Cause Analysis investigating the origin of an avalanche of alarms and fault indications, and in the bottom-up sense, the proactive determination of the user service impacts due to a network fault (e.g. SCADA service for RTUs 4, 5 and 6 are impacted by a major fault on fiber transmission link L7).

6. **Interaction platform for actors and processes** – Sentinel platform comprises incident management and trouble ticketing facilities allowing the assignment of an incident to a person or a team, differentiated service dashboards showing relevant availability statistics to each network user group, mailing facilities for service-related communications, and performance reporting facilities for maintenance management and user/customer contractual relations.

7. **Single access point to vendor tools** – Sentinel framework allows a unique and secure access gateway to multiple vendor-specific tools. The Role-based Access Control implemented between Sentinel Clients and the server can be used to give the authorized maintenance staff individual and logged access to the various configuration and diagnostic tools and crafts existing over the network.

8. **Standard interface points** – Interfacing to other platforms and applications can be performed in a standard way at different levels depending to information exchange requirements:

   a. By linking customized executable scripts to Sentinel's programmable rule-based engines, allowing the execution of user-defined actions conditional to network states

   b. By using web-service interfaces (XML) (push or pull data to another platform (e.g. Grid Management Systems, Security Operation Centre, ...)

FAULT & INCIDENT MANAGEMENT	PERFORMANCE MANAGEMENT
• Technology- and Vendor-agnostic • End-to-end and multi-layer vision • Generic and simple UI (No specific skills) • Enable interaction of O&M actors (including remote clients, field tablets and smartphones) • Assist in network fault root cause analysis • Rule-based notification (event, time, stats.)	• Generate service availability/ outage statistics • Monitor service level agreements (SLA) • Monitor MIB-stored performance data • Service-oriented User Dashboards
CONFIGURATION MANAGEMENT	**SECURITY MANAGEMENT**
• Store basic Network configuration data • Maintain Asset information • Manual data population or CSV import files • Site Geographic location coordinates • Contact Coordinates for incidents, interventions and notifications (user, expert, field staff, ...) • Unified access to vendor tools and platforms	• Role-based access control (RBAC), • Password protection for server access • Operator log management • Authentication through RADIUS server • Secure access for third party systems

Figure 3 – Main functions and features for e-terra Sentinel management framework

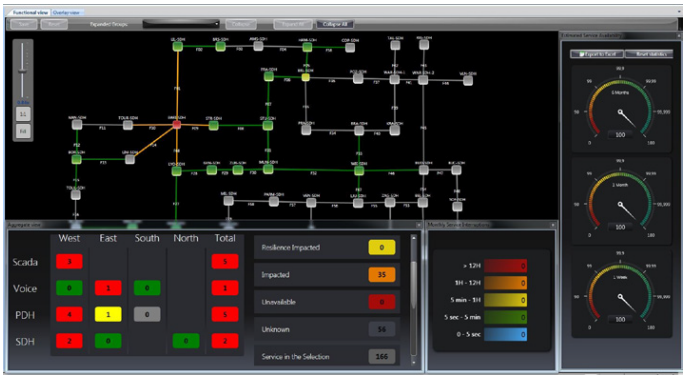

Figure 4 – Example of Sentinel User display with fault and performance monitoring

WHAT IS SMALLWORLD NETWORK INVENTORY?

Smallworld is an information system comprising both Physical and Logical Network Inventories for telecom infrastructures and their constituent equipment, as well as associated tools and applications for streamlining business processes for the planning, engineering, deployment, transformation and maintenance of telecommunication networks. As such, the Physical and Logical Network Inventories provide the following capabilities to the telecom service provider:

- Asset configuration data – Different network equipment types constituting the network can be modelled and consequently used to document the whole network with type and configuration data
- Geospatial visualization of the network – GPS coordinates can be associated to sites and assets and hence enable the presentation of the whole network on geographical maps
- Logical network maps – Logical connections across the network can be stored in the information system with multiple levels of iteration, hence building the logical architecture of the network and its transported services. The Physical-to-Logical link mappings allows the constitution of a network model corresponding to the dependency relationships in the Sentinel overlay model previously described (refer to figure 2).
- Support for network transformation planning – The Network Inventory system enables informed decisions based on complete, integrated, and up-to-date information, transforming the accuracy of network planning, design and engineering, as well as field works based on an accurate view of the as-built network.
- Support for network design – Automatic circuit routing can be performed based on user-defined technology rules. Similarly, the inventory system can perform link bandwidth or system capacity management using the stored network information.
- Asset Life-cycle Management – Keeping a detailed track of the field-installed equipment allows to identify immediately all assets of a certain type or release, installed at a certain date or impacted by a certain obsolescence issue.
- Site installation engineering – The Physical Network Inventory can drill down to the physical infrastructure comprising intra- and inter-site cables, cable ducts, towers, equipment cabinets and distribution panels. It can also document power supplies, air-conditioning facilities and other auxiliary systems relating to the network infrastructure.
- Network protection checks – The network inventory allows the modeling and verification of network protection and diversity schemes using pre-determined rules and operational criteria.
- Mobile-based Work Orders and GIS for field workers - Integration with a Field Force Automation system also provides distinct advantage when it comes to installing new equipment in the field by more effectively managing field mobile workforce.

Figures 5 and 6 hereafter present respectively a functional view of the Smallworld Network Inventory system and an example Physical Network Inventory (PNI) user interface.

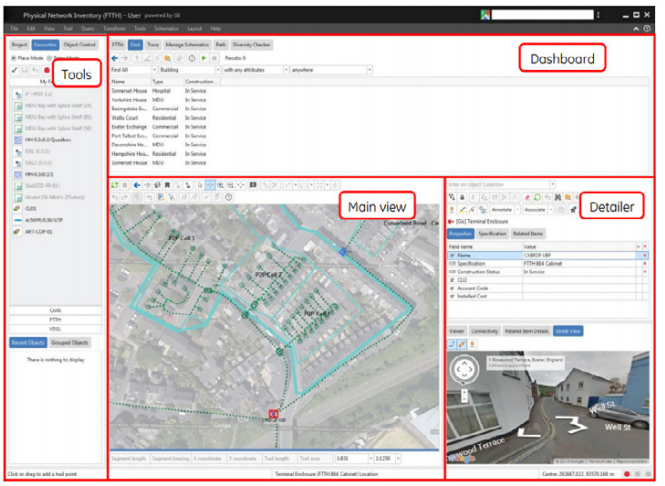

Figure 6 – Example of Smallworld Physical Network Inventory User Display

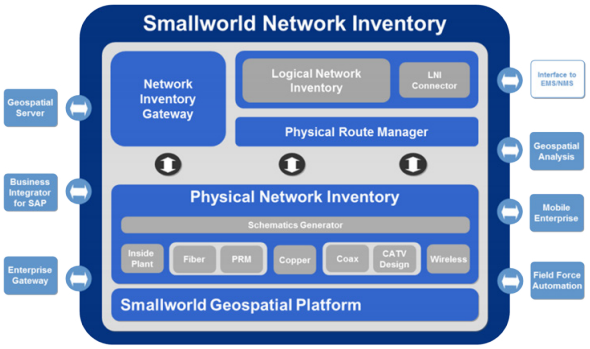

Figure 5 – Smallworld Network Inventory functional architecture

INTEGRATING SENTINEL AND SMALL-WORLD INVENTORY

Sentinel real-time network supervision and the Smallworld network inventory interact in the following manners as summarized in figure 7:

- **Inventory access from the Sentinel framework (Open Smallworld from Sentinel)** – On receiving alarms and events from the network, the network operator can open the Network Inventory on his workstation by right-clicking a network asset or a network connection. In this way, the network operator can get more detailed information relative to the configuration, age and history of a faulty network asset for more informed problem identification and resolution decisions.
- **Populating or updating Sentinel data base** – Sentinel needs to maintain some limited asset and connection data for its own operation and for providing basic network information to the supervisor without any external information system access. However, populating this implicit database requires manual data entry which not only becomes time-consuming in a large network but can also be a source of human error and data incoherence. Using the Smallworld inventory as the information source for network and asset data import allows to simplify data population and increases coherence. Data updating can be performed periodically often at management data administrator's initiative.
- **Future developments** – In addition to these main interactions, further developments are foreseen to be undertaken in future. The following section outlines two major development to store network-captured information and calculated statistical data into the Smallworld inventory information base, and to associate Smallworld mobile work order with Sentinel incident management processes.

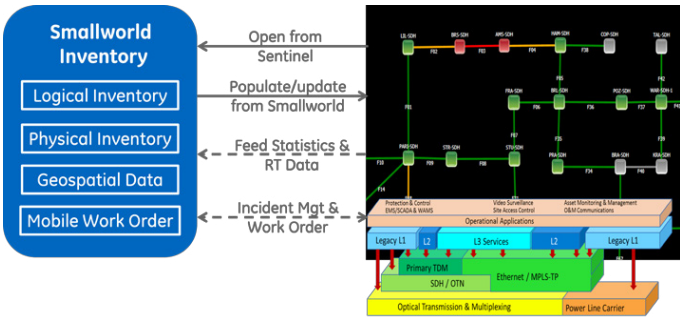

Figure 7 – Smallworld Network Inventory and Sentinel Interaction

FUTURE SENTINEL-SMALLWORLD INTERACTIONS

Feeding Statistics and Real-time Data into the Inventory

Although an inventory's role is not to maintain real-time status information collected by a network supervision system, one can anticipate that network planning tasks performed through the inventory can benefit from statistical data produced by Sentinel. Furthermore, an increasing number of communication systems present automated self-healing or self-configuring features to increase system resiliency, network availability or network throughput. Through its connection to the network components, Sentinel shall capture this configuration data and build in this way the network map at a given instant of time. Statistics and configuration evolution are critical information to be archived for network planning and transformation. This type of Supervision-to-Inventory interaction is a future requirement.

Incident Management and Work Order Interaction

Sentinel framework includes integrated trouble ticketing capabilities for the telecom network. Network supervisors can open an incident ticket when network events are detected, located and pin-pointed across the different layers of network infrastructure. The incident is assigned through Sentinel incident management functions to the appropriate team or person for further investigation and consequent corrective action using vendor-specific tools accessible through Sentinel. Sentinel can further be used for reporting the performed actions and the initiator can then close the incident ticket. Sentinel maintains incident resolution time statistics which can be used for maintenance management and team dimensioning. Smallworld inventory, on the other hand, has the capability of standard work order production which may in future be made accessible to the incident management process in Sentinel. This interaction is also projected for future implementation. Specific work orders for disaster recovery and emergency processes as well as different process automation schemes can be integrated into this future interaction.

CONCLUSION

Managing an operational utility communication network requires permanent awareness of the state of the network at any instant of time as well as physical and logical configuration details. Many operation and maintenance tasks such as fault identification and problem resolution require the association of information captured on the network and engineering information stored in the network inventory. Sentinel-Smallworld association enables the power utility to undertake phased transformations of the network infrastructure and of operational processes in order to deliver Utility-grade communication services in the new digital power grid.

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

GE VERNOVA

GEA-32040-(E)
English
251007