Keep the lights on with improved grid reliability

Through a converged FAN with IP/MPLS for power utilities

White paper

With electricity being central to a modern society, it is imperative to bring highly reliable electricity to customers. For this reason, power utilities are embracing distribution automation (DA) applications such as fault location, isolation, and service restoration (FLISR) and volt/VAR optimization (VVO) to provide intelligent self-healing and automatic voltage regulating capabilities that improve grid reliability and power quality. But this is not enough. DA operations require a highly reliable converged field area network (FAN).

This white paper introduces a converged FAN with the necessary resiliency to reliably carry all FLISR and VVO communications, even during severe weather events when power restoration capability is needed most—so you can keep the lights on.

Contents

The need to improve grid reliability

A fundamental mission of power utilities is to deliver reliable electricity to customers. However, weather events and car accidents do happen, causing faults in distribution grids. Examples include cable failure, insulator contamination and broken utility poles. The end result is service interruption.

According to data collected by utilities in the US, service interruptions from major weather events (snowstorms, floods or heat waves) can last for more than six hours[1]. Service interruptions without major events can for over two hours[2].

Service interruptions impact standard reliability parameters such as the number of customers interrupted (CI) and the number of customer minutes of interruption (CMI). The results are poor system average interruption frequency index (SAIFI) and system average interruption duration index (SAIDI) performance. More important are the economic loss to businesses, inconvenience to communities and hazards to the public, as well as revenue loss to the utilities.

When a service interruption occurs, many power utilities have limited means to locate the fault and shorten restoration time. When a fault is detected, the protective circuit breaker at the substation disconnects power to the entire feeder as a safety measure. To find the exact fault location, utilities need to either dispatch a crew to drive around in the area or wait for affected customers to report the outage—and then restore service. Consequently, with this paradigm, service outage time is long.

While utilities cannot totally avoid faults, they can reduce CI and CMI to improve SAIFI and SAIDI by harnessing the capability of distribution automation (DA) applications. The main one is fault location, isolation and service restoration (FLISR), also known as fault detection, isolation and restoration (FDIR).

FLISR alone is not enough

FLISR plays a pivotal role in improving standard reliability metrics. According to a study conducted by the U.S. Department of Energy, FLISR can reduce CI by up to 55 percent and CMI by up to 53 percent[3].

When a fault occurs and is detected, typically by a SCADA RTU, a line sensor or via the last gasp message sent by Advanced Metering Infrastructure (AMI) meters of affected customers, the FLISR application uses intelligent self-healing capability to start isolation and restoration actions. The FLISR controller, usually integrated with the distribution management system (DMS) and outage management system (OMS), can automatically locate and isolate the faulty section by opening the two normally-closed line switches or circuit breakers adjacent to the fault.

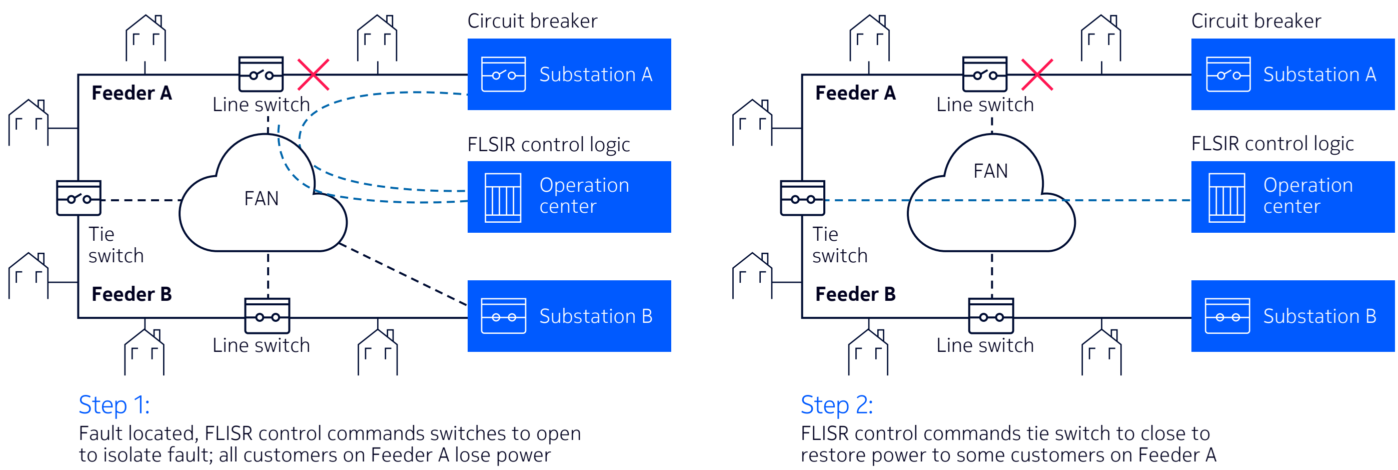
If grid topology allows, the FLISR controller then reconfigures the feeder circuits by closing a normally-open tie switch and transfers affected customers downstream[4] to another circuit powered by another substation.

1 U.S. Energy Information Administration website.
2 Ibid.
3 For more information, read the study on distribution automation conducted by U.S. Department of Energy.
4 This process is also known as load transfer.

Figure 1 shows this self-healing process and the communication paths across the field area network (FAN) to carry out the FLISR operations.

Note that if the communication paths are broken, FLISR operations will be interrupted and will fail to restore power for downstream customers at Feeder A.

Figure 1. FLISR subsystems communicating over the FAN to restore power



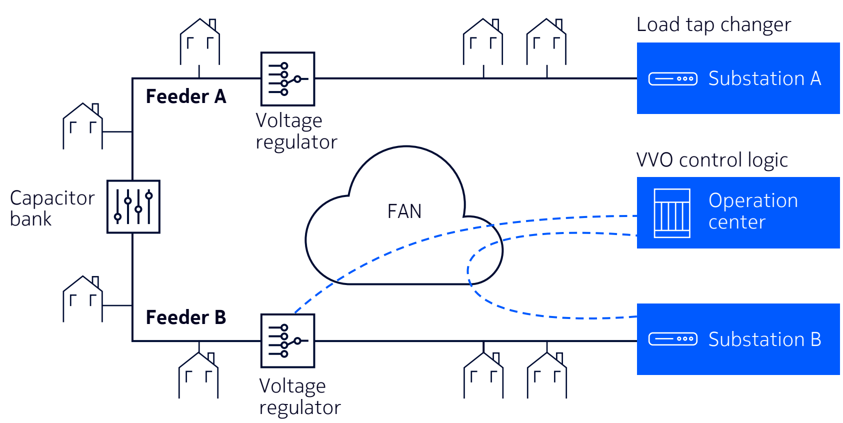
After power restoration (Step 2 in Figure 1), the load level on Feeder B increases, potentially increasing the voltage drop along the feeder beyond the acceptable level of 5 percent of the nominal voltage. This could result in dimmed lights and even customer electromechanical equipment failure. Therefore, it is crucial that utilities constantly monitor voltage level by extracting measured data from line sensors or AMI meters.

Upon detecting voltage drop below the acceptable level, volt-VAR optimization (VVO)—another application integrated with the DMS—can remedy the situation. VVO automatically adjusts the voltage regulator position and load tap changer position to step up the voltage, to return it to the acceptable range.

Figure 2 shows the process and the communication paths taken to carry out the VVO operations.

Note that if the communication paths are broken, VVO will fail to maintain the required voltage level.

Figure 2. VVO commanding voltage regulator and load tap changer to step up voltage



From the preceding discussion, it becomes evident that improving power reliability requires more than just deploying FLISR to restore power for as many customers as possible. Utilities need:

- integration with other DA applications (VVO, AMI, SCADA and line sensors)
- deployment of a resilient, multiservice FAN—because if the FAN fails, grid self-healing fails.

The Nokia converged FAN: Bedrock of a reliable grid

The rest of this paper first provides a brief description of the Nokia converged FAN architecture[5]. It then discusses two essential FAN attributes to enable dependable grid self-healing operations: end-to-end network resiliency and multiservice capability.

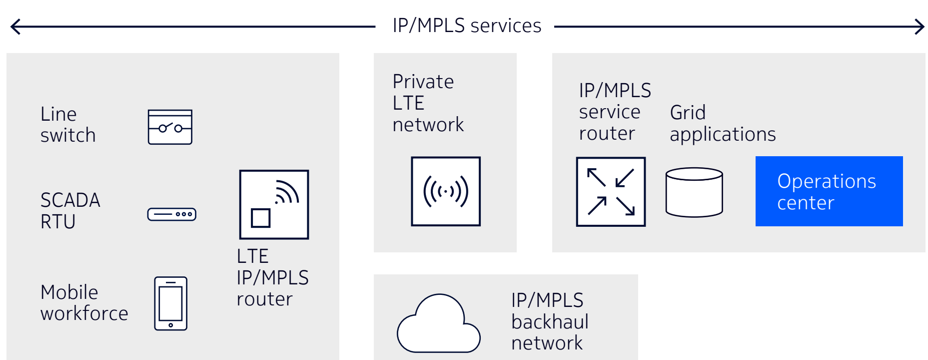
Overview of the Nokia converged FAN

The preceding heading is The Nokia converged FAN (see Figure 3) is grounded in two standards-based networking technologies: IP/MPLS services, which have been widely used in many utility mission-critical WANs, and LTE. The solution harnesses the power of LTE IP/MPLS routers to wirelessly bring IP/MPLS services to utility poles and low-voltage substations that have no network reachability.

Typically running atop a private LTE (P-LTE) network deployed and operated by utilities, the Nokia converged FAN connects intelligent electronic devices (IEDs) or DA subsystems to various DA applications in the operations center. As a converged network, it capitalizes on IP/MPLS service capabilities to carry data from many DA applications with the necessary assured quality of service.

When P-LTE is not an option due to spectrum unavailability or for other reasons, LTE service from commercial carriers is a viable alternative that provides the same functionality[6].

Figure 3. Nokia converged FAN architecture



Strong FAN resiliency

If there is any link failure in the end-to-end communication path, grid self-healing will fail for either of two reasons: DMS and OMS cannot trigger FLISR to remedy circuit faults because they do not receive fault notification from RTUs or smart meters, or the line switches do not receive the instruction to open.

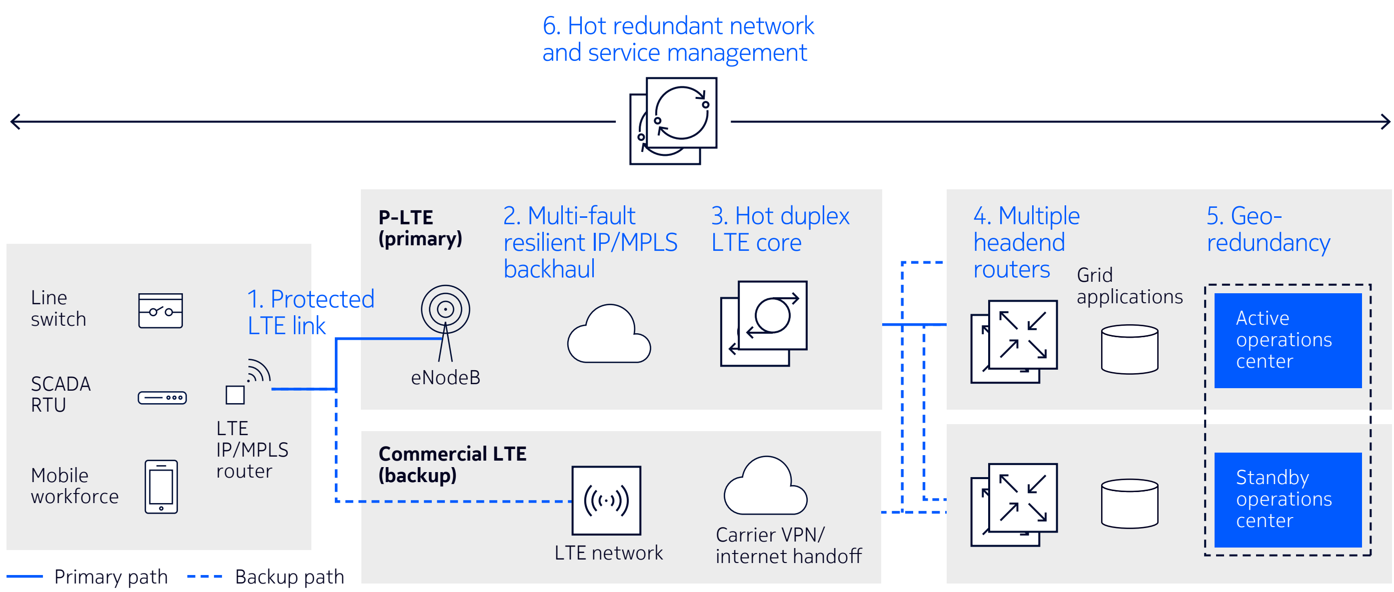
5 For a full description of the Nokia converged FAN, read the white paper "Rethinking the FAN for grid automation".
6 Utilities typically prefer P-LTE because it provides complete operational and maintenance control.

Accordingly, the FAN needs to have a fully redundant end-to-end communication path as well as a feature-rich LTE IP/MPLS router with advanced capabilities and scalability to capitalize on those protective measures (see Figure 4).

The key elements in a resilient FAN architecture are:

1. Protected LTE link
2. Multi-fault resilient IP/MPLS backhaul network
3. Hot duplex LTE packet core
4. Multiple headend routers
5. Geo-redundant operations center
6. Hot redundant network services management.

Figure 4. Key elements in a resilient FAN architecture



1. Protected LTE link

The LTE IP/MPLS router is user equipment (UE) in the LTE network. (As discussed earlier, a commercial LTE network is a viable alternative if P-LTE is not feasible.) The router brings IP/MPLS services to attached IEDs via an LTE link to an eNodeB. If the eNodeB fails, grid communications in the area covered by the failed eNodeB will stop completely, thereby stopping DA operations in the covered area.

Therefore, it is necessary to have a highly available LTE link. Deploying a second eNodeB with overlapping wireless coverage as a backup link is technically feasible but often not economical for a large service area. A cost-effective alternative is to use commercial LTE service as the backup link, as shown in Figure 4[7].

7 When considering commercial LTE service as a backup link, it is important to understand the SLA of and redundancy measures adopted by the commercial LTE operator.

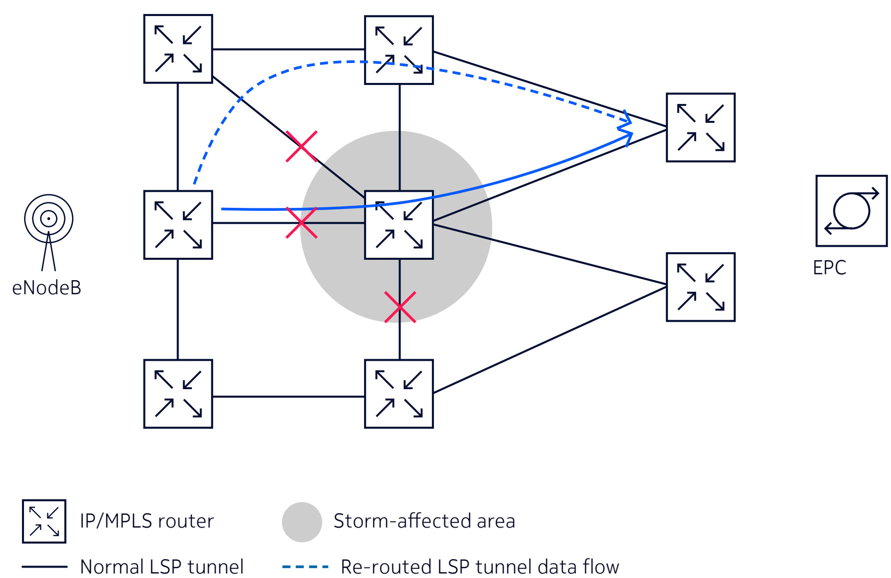
The LTE IP/MPLS router is equipped with two SIM cards to support a dual-homing topology. When the primary LTE network fails, it reconnects to the backup LTE network using the second SIM. Under normal circumstances, the router sends DA traffic over the primary LTE network. The router monitors the operational status of the session between the router and the LTE core, specifically the PDN gateway (also known as the PGW) that connects to a data network attached with DA applications server) in the LTE network. In this way, the router can detect an LTE network fault and switch traffic to the backup LTE network.

2. Multi-fault-resilient IP/MPLS backhaul network

The backhaul network, connecting all eNodeBs deployed in the entire distribution grid service area with the LTE core, is the transport foundation of the LTE network. It is crucial that the network can endure impacts from severe weather events, which can cause multiple network failures over a wide area. This will also disrupt DA traffic in the LTE network, stopping FLISR to restore power. Therefore, multi-fault network resiliency in the backhaul network is critical.

An IP/MPLS backhaul network equipped with network routing information is capable of intelligently rerouting the affected communication path (the LSP) around multiple failures insofar as there is physical reachability (see Figure 5).

Figure 5. Multi-fault-resilient IP/MPLS backhaul network



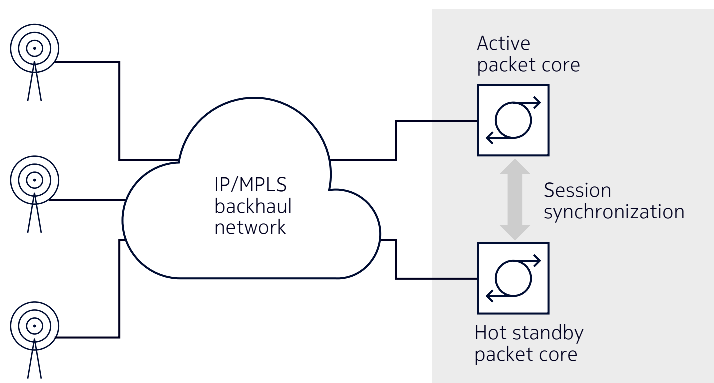
Other IP/MPLS recovery mechanisms such as fast reroute (FRR), which enables the network to consistently restore traffic at SDH/SONET speeds independent of the underlying network topology and size, and pseudowire redundancy are powerful mechanisms to protect the backhaul network connectivity. To further strengthen resiliency, the IP/MPLS network can also harness the resiliency capabilities of the underlying transport, including Ethernet link aggregation and microwave 1+1 protection.

3. Hot duplex LTE packet core

The packet core is the central gateway for LTE radio traffic, managing all communication sessions (called Packet Data Protocol [PDP] sessions) from the LTE IP/MPLS router and other UE. Any core equipment failure renders the whole LTE network out of service, stopping DA applications in the whole grid service area. Consequently, it is necessary to deploy the packet in duplex mode, with an active core and a standby core.

In a typical duplex mode implementation, during protection switching all sessions need to be re-established; this process disrupts all grid communications for minutes. However, hot redundant duplex technology (see Figure 6) allows the active and standby cores to constantly synchronize the state information of all sessions, enabling graceful switching and eliminating any disruption to grid communications.

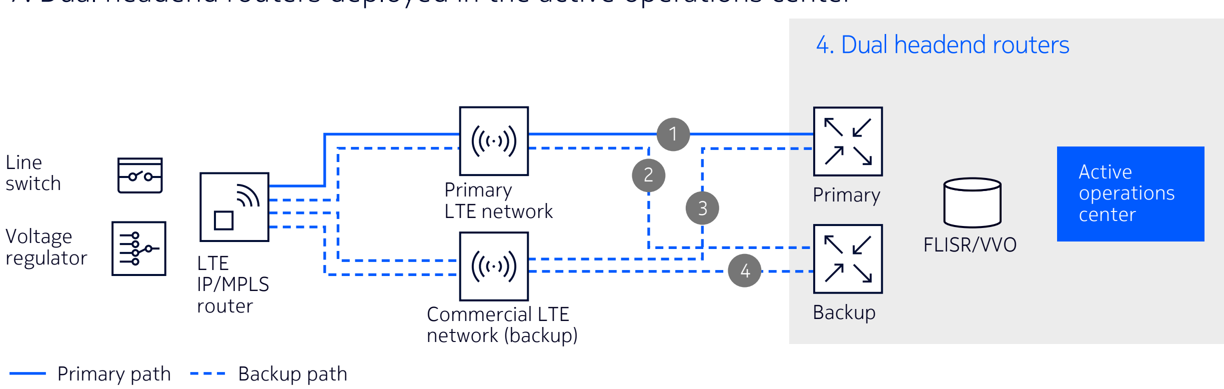
Figure 6. Hot redundant LTE packet core



4. Multiple headend routers

The headend router is located at the operations center, terminating IP/MPLS services that carry all DA application traffic over the LTE network. It is imperative that the headend router be protected with nodal redundancy via backup headend routers located in the active operations center (see Figure 7) and in the standby operations center.

Figure 7. Dual headend routers deployed in the active operations center



It is essential that the LTE IP/MPLS router has the capability and scalability to establish multiple MP-BGP-4 control sessions (4 in Figure 7) with the primary and all other backup headend routers via the primary or backup LTE networks.

The router monitors the operational status of the sessions. When the primary headend router fails, the router detects a status change of session and switches traffic from the primary path, (Path 1 in Figure 7) to a backup path (Path 2 in Figure 7) to connect to the backup headend router.

If a second failure occurs in the primary LTE network, the router will also detect the change of the control session with the backup headend router, then switch from Path 2 to Path 4. This type of multi-fault resiliency is pivotal to ensure that FLISR and VVO are always up and running.

5. Geo-redundancy protection of operations center

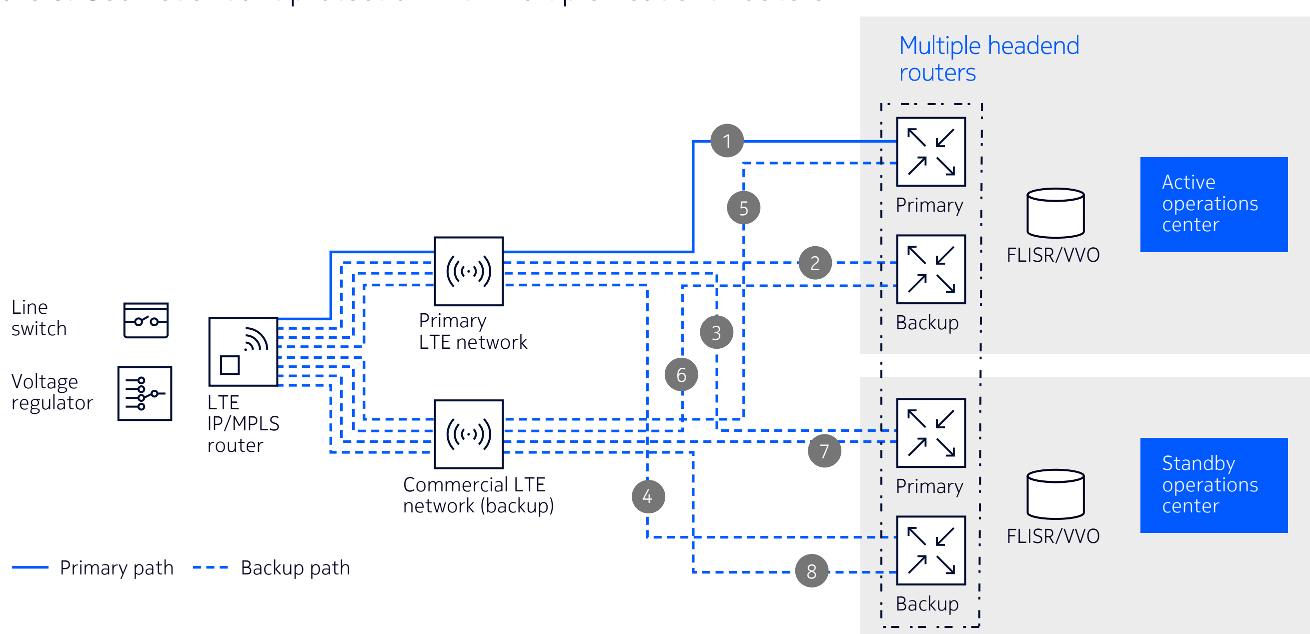
The operations center is the nexus of grid operations where utilities monitor, control and analyze grid operating conditions and also restore outages. Because extreme weather events such as hurricanes and severe flooding are becoming more intense and more frequent, even in urban areas, it is crucial for utilities to have a standby operations center equipped with an identical network and applications environment at a different location.

One key pillar of this geo-redundancy is to extend the multi-headend routers scheme shown in Figure 7 by deploying a backup headend router pair in the standby operations center (see Figure 8). When the active operations center is damaged, impacting all communications equipment, the LTE IP/MPLS router detects the change in the control sessions with the headend router pair in the active operations center. It then switches DA traffic to Path 3 to reach FLISR and VVO applications in the standby operations center.

If the primary LTE network is also struck by the weather event, the router can switch to Path 7 or Path 8 to restore connectivity.

With multiple levels of network redundancy protection, FLISR and VVO can continue to run, to deliver high reliability and quality power.

Figure 8. Geo-redundant protection with multiple headend routers



6. Duplex network services platform

Utilities depend heavily on the network services platform (NSP)[8] to provision and operate their FAN. If the NSP fails, utilities lose oversight of the network status and service performance. Therefore, it is essential that the platform be deployed in hot duplex configurations where the active and standby platforms are synchronized. The standby platform takes over when the active one fails, avoiding disruptions to network operations.

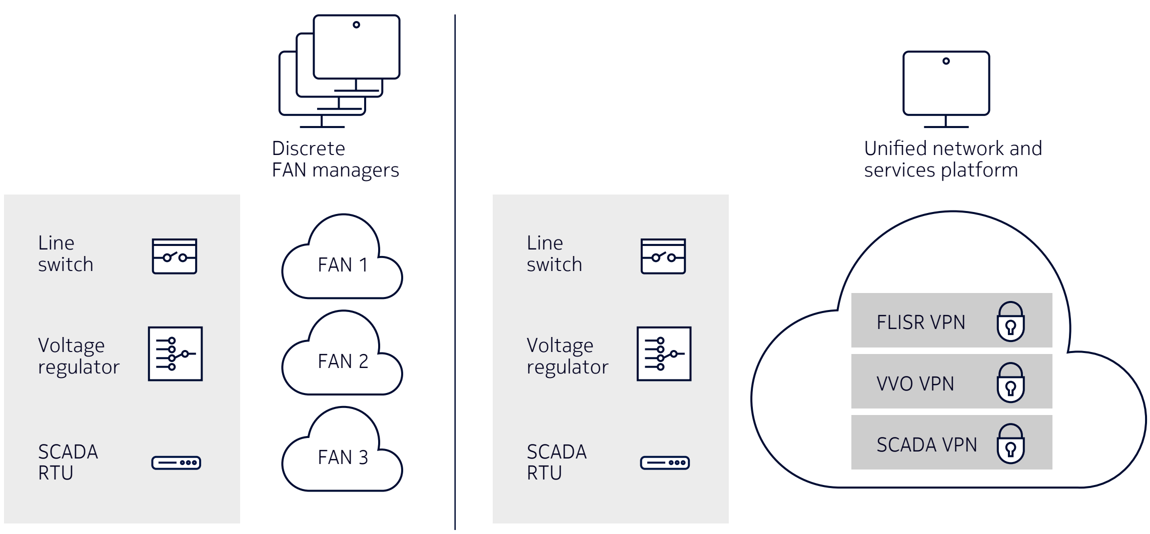
Multiservice FAN

As explained in the beginning of this paper, when FLISR reconfigures a circuit to restore power, the change of load level causes the voltage level to decrease. Therefore, it is necessary to continue to monitor line voltage information with the SCADA system and to trigger VVO to regulate the voltage when required.

Traditionally utilities deploy a dedicated FAN to provision connectivity for one application, resulting in a number of disjointed FANs with discrete network managers (see left side of Figure 9). However, this paradigm does not scale to accommodate numerous DA applications deployed in a smart grid.

The Nokia converged FAN, managed by one network and services platform, harnesses the power of IP/MPLS multiservice capability. It has the scalability to support numerous IP/MPLS VPNs and the services flexibility to support Layer 2 Ethernet VPN, which is ideally suited to carry for IEC 61850 GOOSE traffic, and IP VPN for various DA applications. As a result, the Nokia converged FAN significantly reduces network operations cost when compared with the discrete FAN paradigm. Moreover, with Network Group Encryption (NGE) technology[9], the multiservice FAN also protects grid communications to ensure operations integrity.

Figure 9. Discrete FANS vs. a converged FAN



8 Read the Nokia Network Services Platform brochure to find out more.
9 To learn more about NGE, read the whitepaper “Seamless encryption for mission-critical networks.”

NOKIA

Conclusion

With electricity being central to a modern society, it is imperative to bring highly reliable electricity to customers. Accordingly, distribution system operators are embracing DA applications such as FLISR and VVO, ushering in intelligent self-healing and automatic voltage regulating capabilities to improve grid reliability and power quality. However, DA operations require a highly reliable converged FAN. Equipped with end-to-end redundancy protection, the Nokia converged FAN has the necessary resiliency to reliably carry all FLISR and VVO communications, even during severe weather events when power restoration capability is needed most.

To learn more about Nokia solutions for utilities, visit our Power Utilities web page.

Abbreviations

AMI	Advanced Metering Infrastructure
BGP	Border Gateway Protocol
CI	customers interrupted
CMI	customer minutes of interruption
DA	distribution automation
DMS	distribution management system
EPC	Evolved Packet Core
FAN	field area network
FDIR	fault detection, isolation and restoration
FLISR	fault location, isolation, and service restoration
IED	intelligent electronic device
IP	Internet Protocol
LSP	label switched path
LTE	long term evolution
MP-BGP	Multiprotocol BGP
MPLS	multiprotocol label switching
OMS	outage management system
P-LTE	private LTE
PDN	packet data network
PGW	PDN gateway
RTU	remote terminal unit
SCADA	Supervisory control and data acquisition
SDH	Synchronous Digital Hierarchy
SAIDI	system average interruption duration index
SAIFI	system average interruption duration index
SCADA	supervisory control and data acquisition
SONET	Synchronous Optical Network
UE	user equipment
VVO	volt/VAR optimization
WAN	wide area network

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (February) CID205882