Software-Defined Networking for the Utilities and Energy Sector

shaping tomorrow with you

FUJITSU

One of the challenges for the utilities and energy sector is the constant maintenance and improvement of communications networks, which span multiple domains. These domains mainly include the Core Network (WAN), AN, FAN, and/or NAN. Utilities may own these networks or lease them from service providers; in some cases they have a combination of both. Utilities networks also use a variety of wireline and wireless technologies. The Smart Grids that connect Smart Homes are being built by utilities to collectively shape Smart Cities, and will have to facilitate many new applications and services. The new and/or improved services over utilities networks will include video surveillance, Internet access, power distribution automation, context-aware security, and many more that we have yet to develop. All these new services require collecting ambient intelligence, situation awareness, and frequent communication between equipment pieces and the control center. The Smart Grid will emphasize machine-to-machine communication and big data storage and analysis.

If data centers and public and/or private clouds are not already part of the utilities and energy sector IT infrastructure, they will become so in the near future. However, this market sector has for some time been concerned about the security/privacy of data and the vulnerability of such a complex, heterogeneous communication system. Repeated network and system intrusion attempts are inevitable, but connecting individual instances of intrusion and determining the patterns they follow will help facilitate intelligent prevention of attacks based on solid prediction techniques.

SDN as a Next-Generation Software-Centric Approach to Communications Networks

Current networks are quite complex, costly, and cumbersome. They are based on purpose-built hardware for each network function and use technology-specific connections. For these reasons, a recent paradigm change in networking seems to be picking up speed. Many startups, leading incumbent vendors, and large network operators, are investing heavily in Software-Defined Networking (SDN) as their next-generation software-centric approach to networking.

When it comes to defining SDN, more than one definition is offered by different organizations, but the good news is they all converge on some common points. Among all the organizations, the ONF is the main organization behind SDN [1]. The ONF organizes education about and implementation of this new paradigm, as well as making recommendations for potential migration scenarios [2].

SDN is a programmable open-source approach to designing, building, and managing networks. It decouples network control from forwarding in network devices and offloads its functions to central controller software, called the SDN controller, as shown in Figure 1. Placing the control intelligence into logically centralized SDN controller(s) captures the global view of the entire network and provides the operations personnel with vendor-independent control. An immediate benefit is simplification and consequent cost reduction through consolidation of network devices.

SDN-capable networks will be much easier to manage than networks typically are today. Network administrators will be able to programmatically configure the network at the SDN control layer, instead of having to manually integrate configurations scattered around the network devices. The SDN controller will provide the common network services like routing, access control, dynamic bandwidth management, QoS, storage optimization, and policy management to various utility/energy-specific applications through open NB APIs. SDN's unified control plane allows network abstraction and enables easy and efficient implementation of these applications with required customization and optimization. These abstractions and simplifications will create a fruitful environment for innovation, since turning up new services will be an easier task, once the appropriate software tools have been implemented. The same unified control plane facilitates a virtualized network and makes it possible to "slice" pieces of the physical network or any other hardware along the lines of specific functions, and virtualize these functions. Flexibility is another benefit that SDN offers; mixing and matching of solutions from different vendors will be accomplished more easily with SDN. A summary of how SDN can benefit the current network is provided in Figure 2.

For your convenience, a list of acronyms can be found at the end of this document.

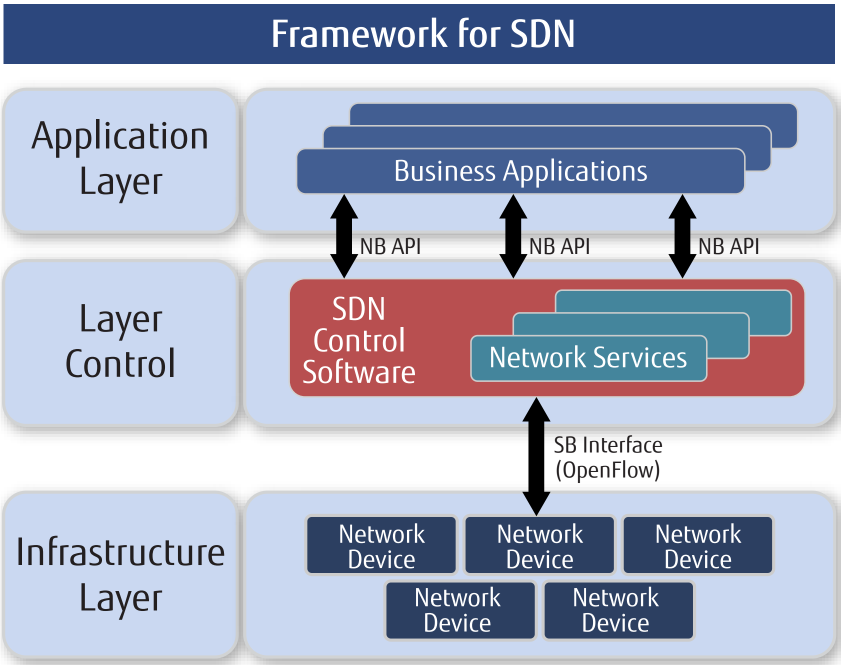


Figure 1. SDN framework

Current Networks	SDN Networks	Benefit
Network provisioning complexity	Self-provisioning	Additional revenue opportunity
Managed network functions	Automated network functions	Reduced OPEX
Technology-specific connections	Technology-agnostic connections	Reduced CAPEX and OPEX
Purpose-built hardware for each network function (routing, firewalling, etc.)	Software-based network functionality	Reduced CAPEX
Multivendor EMSs and their orchestration	Network OS with Southbound APIs	Reduced OPEX
Application-ware networks	Network-aware applications	Innovative applications and increased revenue opportunity

Figure 2. SDN benefits in comparison with current network challenges

Common Communications Networking Challenges for the Utilities and Energy Sector

Utilities and energy companies own and operate multiple networks, as shown in Figure 3, covering large areas and requiring complex management.

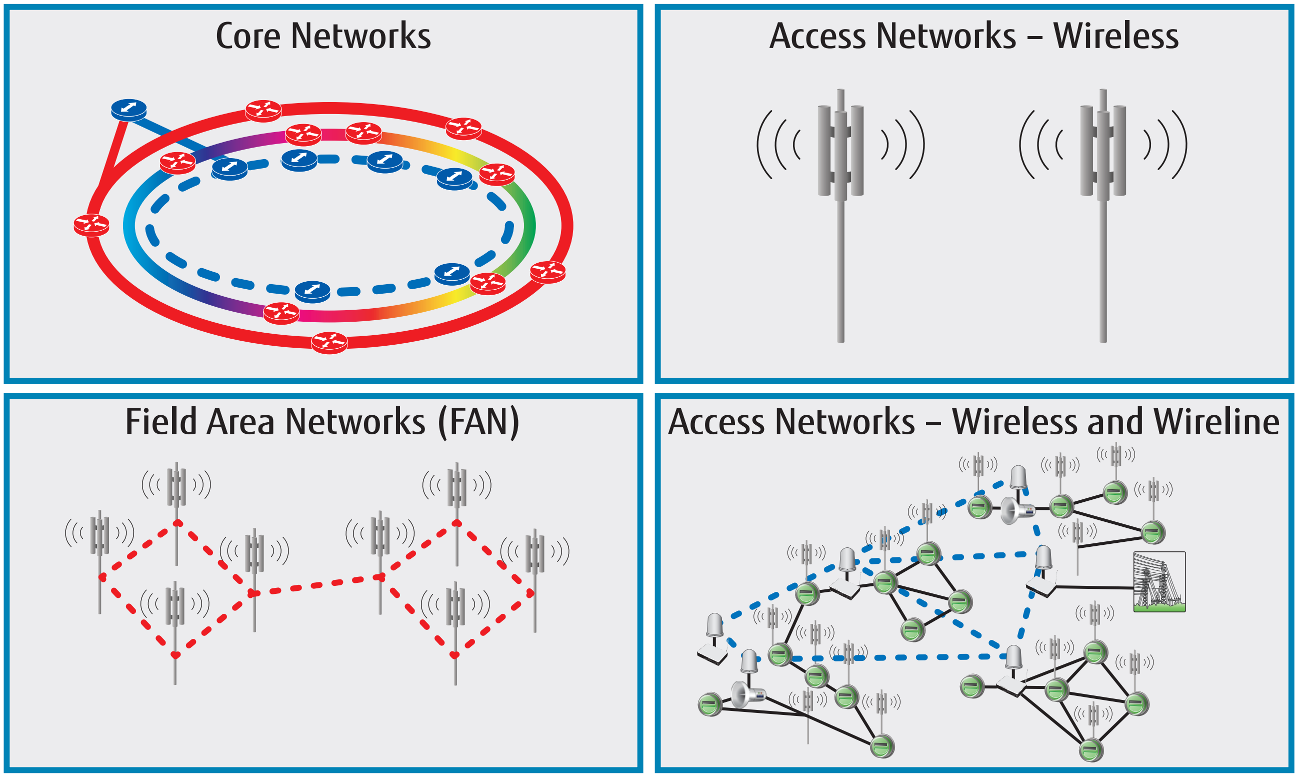

Core Networks
Access Networks – Wireless
Field Area Networks (FAN)
Access Networks – Wireless and Wireline

Figure 3. Typical utility communications networks

Utilities and energy companies also lease connectivity services from network service providers and use multiple vendors with different product life cycles and potential incompatibilities. They have to deal with variety of equipment maintenance and upgrades, which are not easy tasks. Applications and services that run on these networks differ from regular carrier networks. Oil and gas, in particular, have three levels of applications: upstream, midstream, and downstream.

Upstream applications are usually mission-critical emergency response applications and they are near well-heads or entry points in the field. It is desirable to keep these applications on-premises, rather than having them hosted by a third party. Midstream applications are management and maintenance applications for the energy distribution networks and/or vehicle fleets. These applications are lower priority compared to upstream applications. Downstream applications are the retail apps facing end-customers, and internal training apps. These have the lowest priority. All these applications/services need flexible bandwidth for efficient use of network resources.

Resiliency is another important aspect of self-healing networks that need to provide high availability. To accomplish this, millisecond-level restoration should be backed up by controlled delay and jitter. However, it can be challenging to meet these performance benchmarks. The technology adoption cycle for modernization is slower for utilities compared to any other industry due to heavy emphasis on taxpayer investment and sourcing difficulties. For example, a "rip-and-replace" model may not be common practice for the utilities and energy sector because it may not be financially practicable.

Management, maintenance, and migration of the network and its software are another challenge for the utilities and energy sector. These activities are very labor-intensive due to high emphasis on manual configurations, even for a single-domain network, let alone a multiple-domain network. During the process of adopting multiple different networks with a cocktail of technologies in the various domains (WAN, AN, FAN, etc.), the overall topology for these networks changes constantly. Software upgrades are also challenging in such an environment. Regulatory compliance, since it is changing all the time, presents itself as a moving target. Especially in the security area, it is essential to quickly absorb and implement these frequent changes. Mergers and acquisitions are also more frequent these days in every business sector and utilities and energy sector are no exception; therefore, they frequently face the task of merging multiple networks or seamlessly integrating one into the other. New equipment and improved technology should also make their way into the networks of this sector without any disruption to the existing older equipment; which makes interoperability a big concern.

How SDN can Solve Challenges and Enable Modernization

Modernization is a journey for all network operators rather than a destination. As technology evolves, the network needs to implement these changes in the interests of improved functionality and/or reduced costs. Modernization and the implementation of evolved or improved technology allows more services and functionality to be integrated to the network; therefore the network grows.

Current challenges and the push for modernization call for a natural move towards open standards and nonproprietary solutions to reduce OPEX and mitigate the risk of rapid technology shifts. Following this trend, SDN can not only solve some of the network-related challenges facing the utilities and energy sector, but it also presents a solid option for future-proof modernization; see a summary in Figure 4.

SDN, in simple terms, provides a global end-to-end view of the network; therefore, the complexity of multiple domains and networks can be reduced or more effectively managed with this new approach. SDN adopts open standards and introduces technology abstraction, which provides a vendor-agnostic approach to configuring and maintaining various types of network elements. Hardware virtualization is one of the goals of SDN and is used to divide the physical network into virtual slices to ease the burden of managing different networks while using resources efficiently.

SDN will help to connect multiple data centers in different physical locations and make their use efficient. Programmatic network control using SDN provides service abstraction and can simplify configuration activities. Due to its holistic view of network, the SDN-based network will provide superior control of delay and jitter in the network. This will help teleprotection of control traffic, including SCADA. The bandwidth-on-demand feature of SDN will solve the problem of elastic bandwidth need for new and emerging apps in the utilities and energy industry.

SDN's bandwidth-on-demand capabilities will also create opportunities to increase revenue through accelerated service velocity in cases where the utility also serves as a communication service provider in the coverage area. More and more utility companies are functioning as service providers in rural areas.

Fast restoration and self-healing is one performance aspect that may not be implemented in the SDN controller due to its reliance on millisecond-range restoration requirement. This feature may be one of the very few control features that, at least initially, remain resident on the network equipment rather than being pulled into the SDN controller. However, with the anticipated improvements and developments in SDN controller performance, moving restoration and self-healing capabilities into the SDN controller may become possible in future.

In new SDN-based network infrastructure, utility-specific apps on the applications layer will have the opportunity to blossom. These apps could facilitate power/energy peak shaving, analytics of system and customer data, M2M communication, fast restoration from failure, better management of heterogeneous network devices, rapid diagnostics over a large inventory of network devices, distributed automation enablement, AMI network monitoring, and many more.

Utilities Challenge/Need	How SDN Can Address	Outcome
Complexity of multiple networks	Provides global view and control	Simplicity
Multiple vendors and product lifecycles	Software-defined network configuration plus open standards	No vendor lock-in
Data center efficiency	Data center virtualization	Efficient resource use
Large security coverage: ability to control traffic per app	Logically centralized security control and more granular security arrangements	Reduced security breaches
Need for flexible bandwidth – scalability for new and emerging apps	Bandwidth on-demand	Revenue opportunity

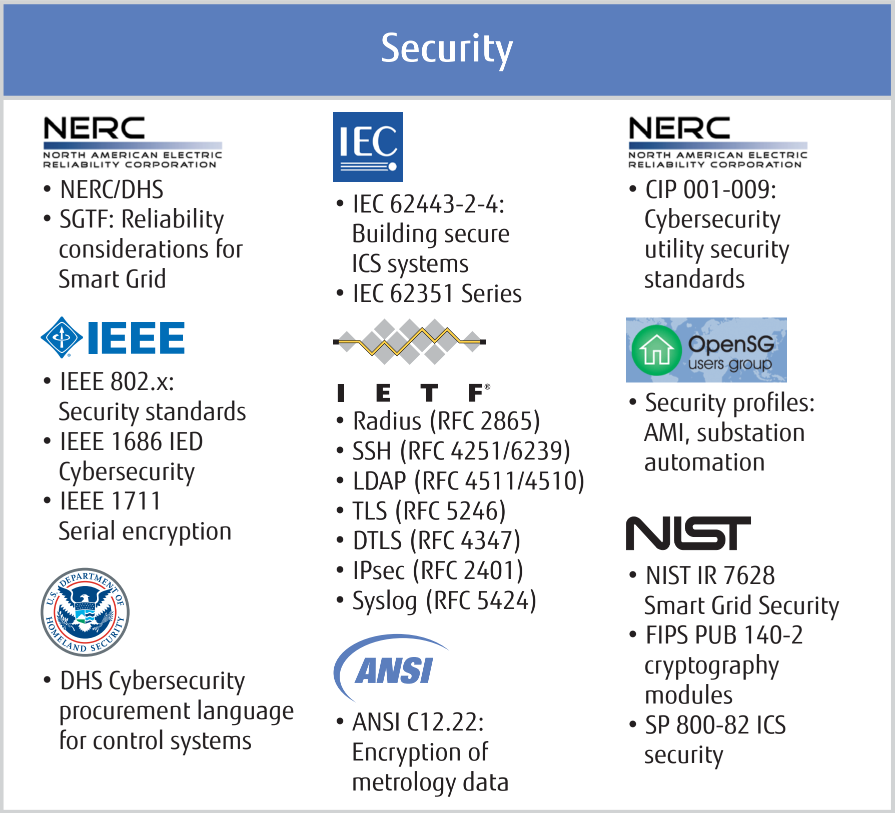
Figure 4. Sector challenges addressed by SDN

Security and SDN

200 SCADA intrusions were reported between Oct 2012 and May 2013 [3]. More than 60% of those intrusions targeted energy and utilities networks. More concerning, these attacks are on the rise, which justifies the recent increase in awareness followed by many conferences and workshops in or around security of critical infrastructure networks and assets. These networks require large security coverage due to their footprint with multiple domains and numerous endpoints. Each one of these endpoints is a point of attack and increases the risk and vulnerability of the system. There are many guidelines, best practices, and standards for security of utilities/energy sector administered by multiple organizations each looking at security from a different angle, as shown in Figure 5.

For a long time we have used the same, strictly defense-oriented technologies and practices for security. This "block everything" mentality has emphasized the use of firewall appliances everywhere in the network. SDN has a potential to change this trend in a smarter way and enable security developers to implement more innovative solutions as applications for perceived threads, since SDN will provide better visibility across the entire network, at both the control and data layers. With logically centralized control, the confusion about where to place the security appliances will end. SDN's security-enabled infrastructure allows network security administrators to route all traffic to a logically central firewall which can be "virtually present" wherever needed in the network. In addition to brute-force defenses, we can expect more intelligent security applications like smarter quarantine systems, faster emergency broadcasts, advanced honeypots, and context-aware detection systems.

The tradeoff between the opportunity that SDN provides for enabling more intelligent and dynamic security applications in the new infrastructure and the risk it poses as a new and unproven technology being integrated to the current systems still remains to be seen. All we know at this point is that the security is a prerequisite for SDN's commercial success, especially for critical infrastructures like utilities and energy sector networks.


Security
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
IEC
IEEE
IETF
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
OpenSG users group
U.S. DEPARTMENT OF HOMELAND SECURITY
ANSI
NIST

- NERC/DHS
- SGTF: Reliability considerations for Smart Grid
- IEEE 802.x: Security standards
- IEEE 1686 IED Cybersecurity
- IEEE 1711 Serial encryption
- DHS Cybersecurity procurement language for control systems

- IEC 62443-2-4: Building secure ICS systems
- IEC 62351 Series
- Radius (RFC 2865)
- SSH (RFC 4251/6239)
- LDAP (RFC 4511/4510)
- TLS (RFC 5246)
- DTLS (RFC 4347)
- IPsec (RFC 2401)
- Syslog (RFC 5424)
- ANSI C12.22: Encryption of metrology data

- CIP 001-009: Cybersecurity utility security standards
- Security profiles: AMI, substation automation
- NIST IR 7628 Smart Grid Security
- FIPS PUB 140-2 cryptography modules
- SP 800-82 ICS security

Figure 5. Security for Utilities and Energy

Conclusion

SDN is coming to networks near you and the utilities and energy sector need to work on how to best utilize the benefits of this new technology for their day-to-day needs in telecommunication networks and share their expertise to shape the future of this new happening.

References

[1] Open Networking Foundation https://www.opennetworking.org

[2] ONF Migration Working Group https://www.opennetworking.org/working-groups/migration

[3] Brute Force Attacks on Internet-Facing Control Systems, ICS-CERT Monitor, April-June 2011, U.S. Department of Homeland Security. http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013_3.pdf (last checked on Feb. 10, 2014)

Acronyms

AMI	Automated Metering Infrastructure
AN	Access Network
API	Application Programming Interface
CAPEX	Capital Expenditure
EMS	Element Management System
FAN	Field Area Network
M2M	Machine-to-Machine
NAN	Neighborhood Area Networks
NB	Northbound
ONF	Open Networking Forum
OPEX	Operating Expenses
QoS	Quality of Service
SCADA	Supervisory Control and Data Aquisition
WAN	Wide-Area Network

FUJITSU NETWORK COMMUNICATIONS INC.
2801 Telecom Parkway, Richardson, Texas 75082-3515
Telephone: 888.362.7763
us.fujitsu.com/telecom