SNC·LAVALIN

# Building the business case for Securing the Digital Utility Transformation

SNC Lavalin – *Intelligent Networks & Cybersecurity*
snclavalin.com/en/inc

# Executive Summary

Power utilities cannot arbitrarily replace the equipment without taking into account the numerous changes facing the industry and digital transformation is at our doorstep.

The digitization of power utilities promises.

> To optimize the supply and demand of electricity;

> To manage the complexity of bidirectional flow of information generated by smart meters and an increasing number of distributed energy resources (DER) and micro grids;

> To offer residential customer load management in support of energy efficiency programs;

> To provide more resilient and self-healing networks against natural disasters.

## Disruptive changes in the energy industry

Such a digital transformation requires capital investments which, if done correctly, can be offset by significant reductions in operational expenses (OPEX).The success of the digital transformation is predicated on a holistic enterprise initiative, as opposed to being viewed solely as an Operational Technology (OT) project).

## The challenge: Return on Investment

Obtaining a strong buy-in and financial support from the executive decision makers is a critical factor for any major undertaking. In its fifth annual State of the Electrical Utiliity Survey, Utility Dive indicates that "justifying emerging grid investments" is a growing issue for power utilities. Accordingly, power utilities may find it difficult to calculate the return on investment (ROI) and produce the strong business case necessary to secure the capital investment required to support the digital transition toward a smart grid.

Real-world experience shows that this can be achieved by adopting a long-term vision and a holistic view of the project, based on three critical building blocks, namely:

> By consolidating existing telecommunications networks onto a single private network;

> Adopting modern OT equipment standards and technology, supporting sustainable and efficient system evolution to a smart grid;

> Designing and maintaining a highly effective cybersecurity program to address evolving threats.

## A single network: a multitude of benefits

Most power utilities have a computer network to support corporate information technology (IT), a network to support the security department's cameras, a private network to support OT, and another one for smart meters. The first step in any digital transformation initiative consists in establishing a reliable and secure private packet switched network for OT. So, why not build a single private network to support everyone?

Power utilities would not only save huge amount of money, they would be in control of one of their most important resources: access to information.

Migrating to a single converged network may reduce the utility's OPEX telecommunications costs by a factor of 3.

## Intelligent substations: The big value nodes

> Intelligent substations will allow power utilities to efficiently manage the intermittent power introduced on the grid by renewable energy sources, optimize the use of energy storage, support bidirectional communications with prosumers, and generate useful data that will be used to perform predictive maintenance on substation equipment.

> Power utilities must invest in scalable technology that will support an open smart grid evolution, as opposed to being tied to proprietary technology.

> One option of the digital transformation is the IEC 61850 standard for substations, which has been adopted by several power utilities in North America and in Europe. This new international standard delivers "plug and play" type communication protocols for intelligent electronic devices at electrical substations.

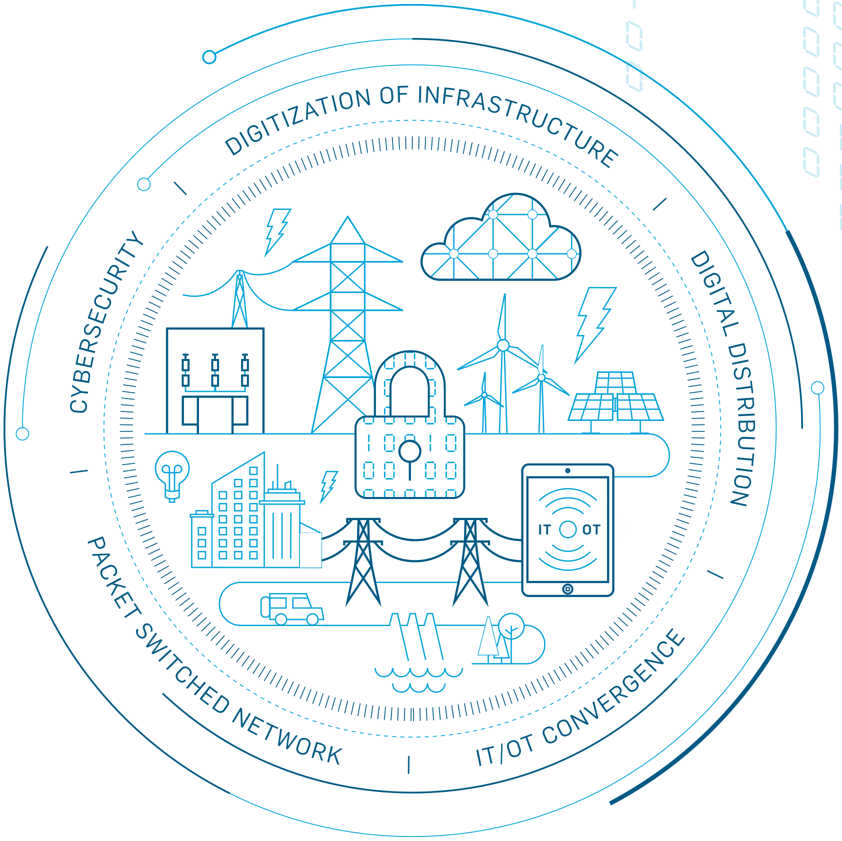
## Maintaining maximum cybersecurity

> When done correctly, utilities can effectively secure their critical infrastructure against new and evolving threats.

> The selection and integration of the right technology, combined with rigorous procedures and culture change, are of prime importance to maintain security risks to a minimum.

The digital transformation will bring about both tangible and intangible benefits, from cost efficiency to increased customer satisfaction, and enhanced load management, grid reliability and resiliency. Such transformation is not without risks, but maintaining the status quo will ultimately generate greater risks.

# A wind of Change is Blowing



Smart grid technology and the rapid adoption of renewable energy are disrupting the power industry. Along with aging infrastructure, these factors are driving utilities to make important decisions on how they will modernize and run their operations. A vast portion of the power utility infrastructure in North America was constructed in the 1950s and 1960s and is nearing "end of life"[1].

Several new variables are drastically affecting the way power utilities manage their grid today, namely :

> Smart meters generate 3,000 times more data than analog meters, which is a source of concerns for privacy advocates.

> To offer a more cost effective service to consumers, online billing connects the utilities' infrastructure to the Internet, with all the security risks that this may bring.

> The introduction of renewable energy injects intermittent power on the grid, which must be offset with large energy storage capabilities.

> With the price of solar panels hitting $1/watt, an increasing number of consumers are generating their own electricity and selling their excess power back to the utility, which not only adds intermittence to the grid, but also complicates the management of the grid.

> Along with the renewable energy trend, the number of microgrids is also on the rise. Although these infrastructures are not subject to NERC CIP compliance, they are often integrated with the power utilities' grid.

**As if this was not enough, blockchain payment technology and NERC CIP data in the cloud are just around the corner!**

Power utilities cannot arbitrarily replace the equipment without taking into account the numerous changes facing the industry.

[1] Gahran A (2018). The State of Electric Utility 2018. *Utility Dive.* Retrieved from https://www.utilitydive.com/library/2018-state-of-the-electric-utility-survey-report/

## A single network: A multitude of benefits

Power utilities must invest in the right technology. The technology must be scalable and adaptable to the smart grid's evolution over time. The migration of data networks (such as those supporting OT, IT, AMI) onto a single converged packet-switched network can reduce a utility's OPEX telecommunications costs by a factor of three. In addition, the converged network provides the flexibility to expand the infrastructure in the future (e.g. following acquisitions) without the need for major re-engineering. This is especially important when considering the merger and acquisition trend in power utilities in the USA. With over 2,200 power utilities in operation across the country, this trend is not likely to stop any time soon!

Given this situation, many power utilities are migrating to a private Internet Protocol/Multiprotocol Label Switching (IP/MPLS) communications network to balance today's business requirements with tomorrow's goals.

Unfortunately, it is common for internal teams to work in silos, thus failing to fully leverage the functionalities of the IP/MPLS network, by deploying parallel networks and having multiple telecom providers to manage.

For example, an OT department may deploy a new IP/MPLS network, while the Physical Security Department continues to pay a Telecommunications Service Provider (TSP) for separate connectivity to support its surveillance cameras and electronic access control devices deployed at substations. Similarly, the team responsible for deploying advanced meters may not take advantage of OT's plans to deploy an IP/MPLS network and will likely continue relying on publicly available telecommunications services. With power utilities facing continuous pressure to reduce OPEX, utilities cannot afford separate communications networks for each application (i.e., for each of OT, IT, Security, etc.). In an IP/MPLS environment, an increase in bandwidth by a factor of 10 to accommodate other applications only increases the cost by a factor of 3 (i.e. not 10 times). This is where significant savings can be made by consolidating networks.

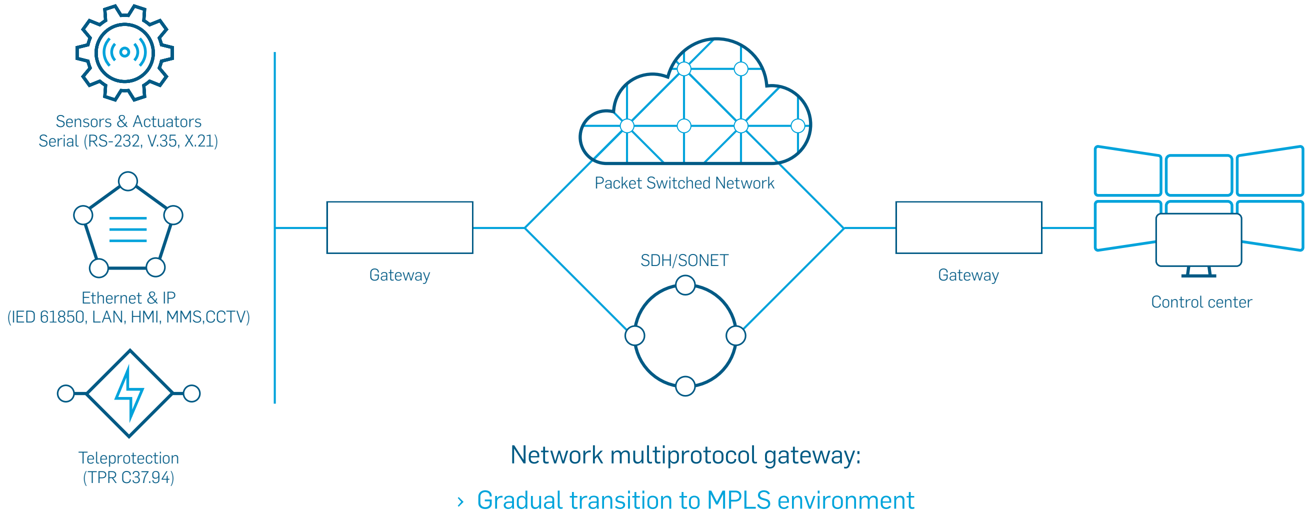
> "Consolidating all the networks onto an integrated MPLS network presents a good opportunity to improve efficiency while reducing costs."

-3X

> "Migrating to a single converged network may reduce a utility's OPEX telecommunications costs **by a factor of 3.**"

> "A converged private network allows utilities to control one of their most precious resources: access to information."

# Transitioning to a Packet Switched Network



Network multiprotocol gateway:

- Gradual transition to MPLS environment
- Low latency

Substation multiservice gateway:

- Unified management (IED 61850, C37.94, RS-232, etc.)
- Secure

## Digital Substations: the Choice of Technology Matters

Having leveraged the consolidation of the telecommunications network, power utilities can then turn to the modernization of substations as another key contributor to ROI. This will not be without challenges, but these will be largely overcome through significant reductions in OPEX in the long run.

Some power utilities may be tempted to continue investing in conventional technology or to simply replace obsolete analog devices with digital equivalent (i.e., digital status quo). This approach limits grid efficiency improvements and the ability to migrate to a true smart grid. The digital transition must be viewed as a long-term evolution, versus short term fixes, with investments made in scalable technologies that will allow utilities to adapt to changes in the future.

## The benefits of the IEC 61850 Standard

One option of the digital transformation is the IEC 61850 standard for substations, which has been adopted by several power utilities in North America and in Europe. The benefits of IEC 61850 to utilities include accelerated project delivery, reduced installation costs and enhanced substation and grid management (by integrating the increasing number of DERs and supporting bidirectional communications with customers). Furthermore, not only does the standard allow the remote support and troubleshooting of faulty equipment, but the big data captured from various sensors and EID will, among other things, enable predictive maintenance, thus reducing power outages and prolonging the life of equipment.

"Power utilities must invest in scalable technology in order to adapt to the smart grid evolution over time."

"Digital transition must be viewed as a long-term evolution, versus short term fixes, with investments made in scalable technologies that will allow utilities to evolve."

## The IEC 61850 Standard - Bringing "Plug and Play" to Substations

It is important to note that the major cost component of technology migrations is configuration and documentation, not the equipment itself. IEC 61850 simplifies and standardizes system and device configuration, and on going data management. It is built on an object oriented and hierarchical data model, which contains data models of most substation automation functions, including those designed to support renewable energy integration, and other DERs. With this "plug and play" type feature, the initial data gathering process and automatic configuration are initiated as soon as a device is connected.

Many substations have been highly customized over the years and this lack of standardization has resulted in a significant increase in operational overhead.

It has been estimated that the use of standardized substation configurations, combined with the IEC 61850 functionalities, can diminish the time needed to configure IEDs by 75%[2] while considerably reducing configuration errors.

## Industrial Internet of Things (IIoT)

Older proprietary protocols for communication in substations, including Profibus, IEC 60870-5, DNP3 and Modbus, lack the standardized representation and organization of data in substation devices at the application layer. Not surprisingly, the introduction of Industrial Internet of Things (IIoT) devices using these legacy protocols is not a viable option. The introduction of IIoT devices will considerably increase the volume of data generated by substations, which means that Supervisory Control and Data Acquisition (SCADA) systems could become the bottleneck to the smart grid evolution. IEC 61850 addresses this problem by establishing peer-to peer "virtual connections" via Generic Object-Oriented Substation Event (GOOSE) messaging.

> "The major cost component of technology migrations is configuration and documentation, not the equipment itself."

### Opportunity

"The use of standardized substation configurations, combined with IEC 61850, can reduce the time needed to configure IEDs by 75%[2]."

-75%

This feature eliminates the latency introduced by SCADA systems and allows all types of controllers, IEDs, and intelligent subsystems to cooperatively communicate between themselves over the substation TCP/IP network.

IEC 61850 also makes any software upgrade much easier to perform, reducing costs and facilitating security patch management. To that end, the IEDs compliant with IEC 61850 can be upgraded over time without the need to replace the equipment or redesign the substations. With this technology, the service life of the equipment is mainly driven by the vendors' capability and willingness to support the equipment during its lifetime, not the obsolescence of the equipment itself.

The migration toward an IEC 61850 environment will not be without hurdles, such as the personnel's preference for conventional and familiar legacy equipment. Given these human resource issues, change management must be factored into the project plan.

## Maintaining optimal cybersecurity

Utilities may perceive that the convergence or networks, the introduction of numerous IIoT and AMI devices increase their exposure to cyberattacks. Although these concerns are legitimate, utilities can defend against new cyberthreats using an effective defense-in-depth strategy.

The IEC 62351 and DNP3 SA v5 security standards[1] address four major requirements for end-to-end securing data communications and data processing: confidentiality, data integrity, authentication and non-repudiation. Among others, they offer protection against:

> Eavesdropping.

> Man-in-the-middle attack[3].

> Spoofing[4].

> Replay attack[5].

Relying on well-known Public Key Infrastructure (PKI) standards for the management of digital certificates, IEC 62351 provides many important security functionalities essential to support a smart grid, such as:

> Cryptographic key management.

> Authentication of users and devices.

> Authorization of users and devices based on pre-established roles and functionalities.

> Operation integrity using digital signatures.

> Confidentiality (used mainly to protect encryption keys).

Therefore, just because substations are going digital does not necessarily mean that they are more vulnerable to a cyberattack; once again, the selection and integration of the right technology, combined with rigorous procedures and culture change, are of prime importance to keep security risks to a minimum.

[1] These two standards are fully compatible and interoperable

[2] Shoene J. and Humayun M. (2017) Advanced Protection and Control for Smart Grid. New York, NY: CRC Press.

[3] An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

[4] A situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate access to systems.

[5] A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated to affect the operation of industrial control systems.

# Use case:
# ABC Power inc.

You are tasked to build a business case for your company's investment in emerging network and substation technology, and need to determine the ROI. The first question that needs to be answered is who are the main consumers of data network bandwidth in the organization? Invariably, IT, OT, Security and Advanced Metering end up at the top of the list. How much are they each consuming and paying for these services? How much would we save by migrating all these applications onto a single IP/MPLS network? What are their specific technical requirements or constraints (latency, bandwidth…)? What benefits can be derived from this approach? Let's analyse a typical power utility case study.

## ABC Power Inc. Profile

- ABC Power Inc. is an electric distributor whose transmission and distribution network has recently grown to include 300 substations through the acquisition of smaller electric distributors in the USA. The company now serves two million customers.
- Legacy analog IEDs, which are connected to a TCP/IP LAN via serial-to-Ethernet adaptors are still in service and need to be replaced.
- Each substation is connected to a privately owned OC-192 SONET fiber-optic network (10 GB). The network does not scale well and major work needs to be done each time an acquisition is done.
- The Physical Security Department monitors the security cameras and remotely manages badge readers at the substations via leased lines provided by various TSPs (multiple contracts to manage).
- A smart meter pilot project has been initiated and the Wide Area Network (WAN) supporting the Advanced Metering Infrastructure (AMI) is an IP/MPLS network leased from a TSP. The quality of service of the network offered by the TSP is "best effort".
- The IT department leases IP/MPLS network services from a major TSP to interconnect all its office buildings. To reduce costs, there is no Quality of Service (QoS) offered by the TSP, which means that the existing video conference capability is unreliable.

# Deploying a common IP/MPLS network

An upgrade of ABC Power's existing 10 GB private SONET to a 100 GB core IP/MPLS network will bring considerable benefits, including:

> Generating an ROI within five years following the consolidation of the networks. Although training would be required, the IP/MPLS network would not require additional OT but personnel to manage it.

> Supporting the company's plans to continue acquiring power utilities, by providing the ability to quickly add new substations without the need for redesigning the telecommunications network.

> Having total control over the quality of the services provided (i.e., not based on the "best efforts" of a TSP), leading to a more reliable service offered to customers.

> Providing QoS to IT to improve the quality of their video conferencing.

> Providing the ability to store data generated by the security video cameras in a centralized data center, thus eliminating the need to maintain video servers at each substation (i.e., patches, anti-virus, software upgrade, repair, etc.).

> Creating a mirror site and a recovery site for the operations center, thus increasing the resilience of services provided in the event of incidents or major regional disasters.

Over time, the central management and troubleshooting of IEC 61850 compliant IEDs generate considerable OPEX savings and efficiency improvements.

# Replacing the IEDs

The main focus is on the old legacy IEDs that must be replaced over the next few years. When it comes down to how much effort it takes to commission substations with IEC 61850 technology vs. other protocols, the answer is simple. Cost over time for support and maintenance makes IEC 61850 a clear choice.

Round trips to substations represent a frustrating loss of service time and manpower. With IEC 61850 compliant equipment, troubleshooting can be done remotely at the Operations Center. From there, the problems will be diagnosed precisely and technicians will be sent to the substations only when it is necessary to replace a faulty component. Furthermore, to avoid potential problems during installation, the spare equipment will have been configured and tested in a pre-production environment. The result: the response time is improved dramatically, while reducing the number of technicians and subcontractors.

Many types of IEC 61850 devices are supplied by various manufacturers. The use of a standard architecture for the substations can significantly reduce recurring engineering efforts for ABC Power.

The replacement of obsolete IEDs by IEC 61850 compliant devices will bring tangible and non-tangible benefits, such as:

> Configuring substation IEDs more efficiently, with fewer errors;

> Reducing the physical space needed in the control house by up to 30%.

> Centrally managing and troubleshooting the devices will reduce the need for technicians going from station to station with laptops and test equipment.

> Taking full advantage of the security features of the IEC 61351 standard will create a more secure environment.

> Leveraging peer-to-peer GOOSE capabilities, will allow the partitioning of certain applications into cooperative modules and their distribution among different IEDs. This provides unprecedented flexibility to manage the power utility's information and automation environment, while reducing potential bottlenecks by the SCADA system.

# Conclusion

The digital utility transformation will bring both tangible and intangible benefits, from cost efficiency to increased customer satisfaction, and enhanced load management, grid reliability and resiliency. Such transformation is not without risks, but maintaining the status quo will ultimately generate greater threats.

A successful transition to a digital environment is not limited to technology; a holistic strategy must be developed to reap maximum benefits of the transformation.

This endeavor requires careful planning, taking into account many critical variables such as cultural change. And while justifying emerging grid investments is seen as a growing issue for power utilities, this document has identified the key elements of a stratey for building a strong ROI to support your business case, making it much easier to sell to the executive decision makers!

Intelligent Networks & Cybersecurity
CLEAN POWER
Email : INC-RIC@snclavalin.com
Tel CND: 514- 392-3000
Tel USA: 713-744-6100 ext 58730

snclavalin.com/en/inc

IMPRIMÉ AU CANADA     CONCEPTION : TMDESIGN.CA

# SNC-Lavalin
# Intelligent Networks & Cybersecurity

Founded in 1911, SNC-Lavalin is a global fully integrated professional services and project management company. From offices around the world, SNC-Lavalin employs 53,000 employees with a strong presence in the United States (86 offices and over 6,500 employees).

Intelligent Networks & Cybersecurity team provides comprehensive end-to-end project solutions including: consulting, studies, design, work surveillance & inspections and support services to procurements.

Our expertise covers different sectors such as: Cybersecurity, Physical and Site Security, Telecom Networks Transition, Protection & Control / OT/AMI.

This broad expertise makes us a compelling partner with solid knowledge and insight that enables you to develop effective and proactive long-term strategies on the challenges faced by digital age utilities.

Visit us at snclavalin.com/en/inc

SNC·LAVALIN

Securing what matters

SNC Lavalin – *Intelligent Networks* & *Cybersecurity*

snclavalin.com/en/inc