DEVELOPMENT OF REMOTE MAINTENANCE CENTER FOR SUBSTATION AUTOMATION SYSTEM

Author: Abdullah A. Al- Jahil,
National Grid, Saudi Arabia,

This white paper is intended to provide all users with a practical selection guide and strategic plan of developing remote maintenance center for substation automation systems. By taking National Grid Saudi Arabia as a case study to demonstrate its experience in the automation environment and approach to building remote maintenance center. This paper will be also cover the technical aspects according to the standards. It will focus on the existing advantages, and the remaining obstacles that are likely to occur with comprehensive guidelines of recommendations and action plans. Nevertheless, utilities and energy sector providers still face concerns with high capital and operational costs in their business. So, the paper will consider estimating expected capital fund for this investment and the saving return in operational expenses by providing real statistics from fields which can support decision maker to choose which option is best fits for their business style.

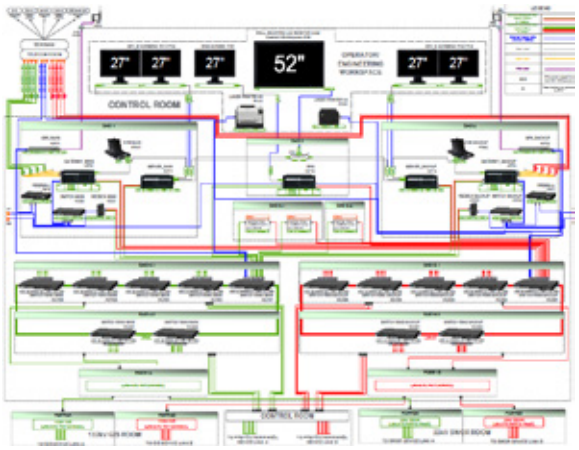
About National Grid Saudi Arabia

NG ASSETS	TOTAL
SUBS SUBSTATIONS (380 KV – 110 KV)	1010
PEAK LOAD (GW)	62.260
SUBSTATION AUTOMATION SYSTEMS (SAS)	572
FIBER OPTICS CABLES (KM)	52.395
WIDE AREA NETWORK (CORE)	51
WIDE AREA NETWORK (CE)	761

National Grid SA (NG) is a power utility responsible for the transmission of electricity across the Kingdom of Saudi Arabia (KSA). NG uses transmission voltages of 380KV, 230KV, 115KV, and 110KV and has more than 1010 substations, transformers, kilometers of transmission lines, and over 52,000 kilometers of fiber optic cables. NG faces many of Saudi Arabia's specific electricity sector challenges that require migration actions to meet the unbundling of the sector, peak electricity demand and quality of service. Power utility networks have always been inherently different from traditional corporate networks. The bulk of their infrastructure is dedicated to communicate with industrial equipment using various SCADA, SAS and smart grid protocols.

Table 1: NG assets [3] Smart Grid Envision By Abdulaziz A. Al-Sultan (Nov 2013)

Substation automation system (SAS).



In 2010, NG adopted SAS in their substations as a remote digital control system by employing the international IEC 61850 standard, which dominates the integration of all field applications. The SAS is a digital control system that is efficient, reliable, resilient and responsive. A real-time monitoring and control system has complex interlocking and sequence control requirements. The SAS is Ethernet-based and connected to one or several energy management systems by using serial or Ethernet protocols such as IEC 101 and IEC 104 through a complex cloud of a telecommunication network.

Remote maintenance center

Substation Automation systems are widely used for the purpose of control, protection, monitoring, communication etc. in substations that are in long distant locations. This often leads to problems when needing to diagnose, investigate and solve errors in the event of a fault. Complete remote support and monitoring of the system process is now possible. Thanks to developments of the technology, Remote maintenance describes remote access to automation system for fault diagnostics or for all software maintenance and administration purposes.

Remote control center

Energy management system (EMS) is widely used to display all substation parameters in real-time. It describes the remote monitoring and controlling of physically separate system parts by

means of data transmission. Measured values and control commands are transmitted over long distances and visualized, processed, and stored in a control center. The required information of circuit breaker statues , for example, Figure2: Sample of Remote control Center can be archived centrally for many years. Data can be transmitted securely over wide area networks (WAN), with discrete digital and analog signals. Recently there has been a clear move away from serial transmission paths toward IP-based communication.

Differences between remote control center and remote maintenance center.

In industrial communication, there is a vast difference between remote control and remote maintenance, even when using identical technology. This often leads to confusion when it comes to selecting the right communication media. The particular features of the different applications are therefore described below.

	Control center	Maintenance center
Function	Controlling / monitoring the power network	Administrating and maintaining the Automation system
Communication media	Serial, Ethernet, Radio	Ethernet
Operator	Power Dispatcher	SCADA Engineer
Objective	power Control & fast restoration	System administration & recovery control

Table 2: Differences between Remote control center and Remote maintenance center.

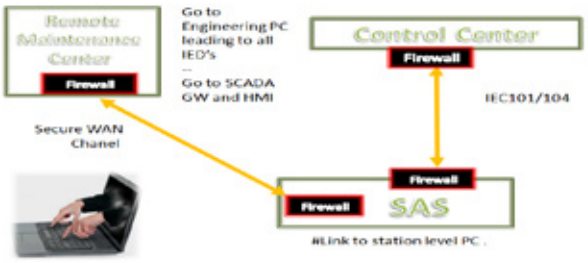


Figure 3: Automation system communication with Remote control center and Remote maintenance center.

Need and importance for remote maintenance center

3.1 Responding to the emergency situations

In case of system failure. System engineer needs to go to substation , to solve the fault and restore the system to be in service and available for power dispatchers in short time. Any delay might happen of recovering the system , it may cause a negative consequences or real damages to the network due to unavailability of the information in control center. This delay can happen due to many reasons for instance traffic jams in big cities and far or isolated substation locations which make reaching substations quickly very challenging or others.

3.2 Increasing in operational expenses

By managing the automation systems in wide - coverage areas locally and manually the cost of maintenance will increases dramatically due to traveling expenses, time required for system restoration, needed number of employees and required tools such as cars and others. The chart below describes the National Grid SA master plan for Smart Grid transition.

Conventional Systems	Automation Systems	New Technologies
(RTU, DSM, SOE, WS and others)	(GTW, SRV, EWS, SWITCHES, BCU, IED)	(Digital Substation, Smart grid initiatives)

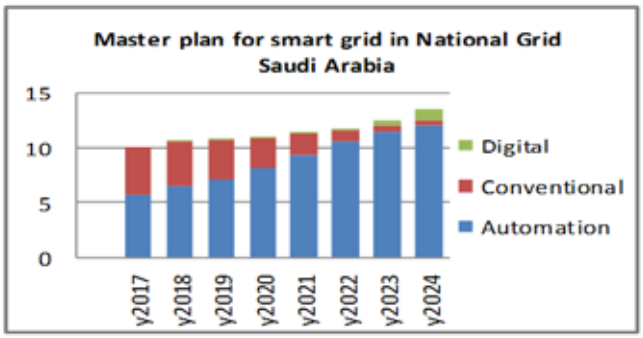


Chart 1: Installation of SCADA systems in Transmission Substation from (2017 to 2025).

Chart trend analysis (2017-2025)

Automation System (Statues of use: Sharply increasing)

The use of SAS in National Grid SA's substation will keep increasing to be 75% from the total number of substation, which may reach 1000 out of 1200 Substation.

Conventional SCADA system (Statues of use: decreasing)

The use of Conventional SCADA system in National Grid SA's substation will keep decreasing to be 19% from the total number of substation, which may reach 250 out of 1200 Substation.

Digital Substation system (statues of use : slowly increasing)

The installation of Digital system in National Grid SA's substation will slowly increase to be about 10-20 out of 1200 Substation. Based on National Grid SA master plan for smart grid transition and the chart trend analysis, National grid will rely on the automation system as controlling and monitoring systems in its substation. This move was decided to get advantage from the technology by utilizing the features offers by automation system. The main concern ware enhancing the efficiency and reliability and decreasing the capital and operational cost.

3.3 Complexity of technology in various fields

NG SAS Design components	Total # In Ave
Computers	6
Managed Network Switch	25
Printer	3
Bay Control Unit	20
IED's	100
Type of Users	12
Protocols	5
Applications	50

Today's industrial product show a strong increase in functionalities and complexity. Maintenance engineer faces huge difficulties of mastering all different aspect in technical part. Dealing with emergencies situation under time pressure, criticality and sensitivity make it much worse. Think of Automation System, which is a set of protections, automation, data networks and cyber security. The combination of which makes it much more difficult for quickly identifying, isolating, diagnosing, and repairing any faults. The SAS is set of IED's (protective relays, bay controls, etc), computers and network devices from several manufacturers, all connected via network redundant protocols as PRP and HSR. Other communication protocol include IEC 61850, T101, T104, SNMP and ANTP.

Table 2: NG SAS average # of components

Basic physical requirements for Remote Maintenance Center:

4.1 Maintenance Workstations

Minimum System requirements for effectively running the maintenance work station. The hard disk space grows overtime based on the stored data. More RAM space and high end processors are required depending on the Support Load and simultaneous access load. Industrial PC's with all software of :HMI, BCU, SWITHES, GTW, SRV,IED's AND Other tools need to be installed and licensed.

4.2 Secure Platform

International industrial cyber security standards define specific security standards based on the level of security needed as well as system criticality and locations . Securing the system from any access without authorization is always a need and big concern. physical access through biometrics, card readers, as well as padlocked Only authorized and authenticate engineers are allowed to access the remote maintenance center and systems work station.

4.3 Wide Area Network

WAN is recommended in applications where data from IP devices is transmitted. WAN describes an Ethernet network and supports the TCP/IP modules. For Automation remote access the activation of IEC 104 is required for application that used by a large number of devices. Particularly suitable for monitoring, operation, and data acquisition as it can be easily integrated into OT networks.

The associated challenges include:

Cyber security threats and strict polices for remote connections.

Communications failure.

Lack of experts and qualified engineers to run and operate the remote center due to diversity of systems, functions, designs, architectures and vendors.

Organization culture and change resistance to use new concept of technology by using Ethernet communication protocol IEC104.

Project budget and capital funds.

Absence of real model and few cases with remote maintenance centers exist in utilities worldwide.

National grid Action plan and guide line for implementation.

Global Improvement of Cyber Security measure at National Grid SA Industrial Control System.

The need and importance for control system security in utilities is great, The impact of a possible power network failure on the Kingdom of Saudi Arabia and on the reputation of NG made NG take responsibility for power network security by taking action for massive improvement program to make the power network more reliable and more secure. They reflect international standards and common best practices. And set of initiatives including master plan have been identified by NG to address the relevant and critical areas of improvement with different levels of priority and complexity. The security heat map for SAS below highlights the domains with number of areas of improvement to include suggested mitigation strategies in each vulnerability category. However, some of these actions have been already implemented in the field.

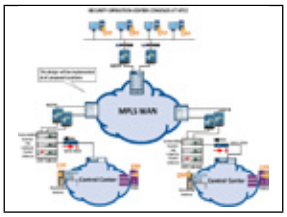
Figure 3: Heat- Map for cyber security improvement

Enhancement of Physical and environmental access: This includes physical access through biometrics, card readers, as well as padlocked of the automation panels and server panels.

Monitoring: This includes systematic logging and SAS event alarming, and auditing, leading to the ability to track different SAs security issues and particularly allowing for traceability of access and actions. It also includes centralized monitoring of network devices and server health.

Improvement of asset management: This includes reinforcement of the asset management and systematic inventory list applications, and prompt recovery from an incident by having backup and restoration policies in place. SAS asset life is prolonged by clearly defining the maintenance strategy, including the adoption of a patch management process.

Improvement of NG processes: This includes structuring incidence response team processes and responsibilities among NG and its stakeholders in the case of cyber-attack, as well as a large deployment of cyber security, and comprehensive trainings to ensure awareness among employees of NG and its stakeholders.



Centralized cyber security operations center: This can be used to manage all NG events to control, monitor and have the ability to better react and defend in the case of an attack. In particular, this SOC should be able also to perform some preventive maintenance and fine tune emergency plans, release reports, and deliver additional basic security services such as security infrastructure management, security intelligence, penetration testing, as well as advanced services like security analytics and cyber intelligence.

Figure 4: Sample of Security Operation Center SOC

Firewall upgrade: Upgrading to the next-generation firewall technology, which can provide more complex security configuration and management.

Forming regional and local maintenance teams.

In case of communication failure or hardware problem, the operator of remote maintenance center will not be able to access the system. That's why there is a need for regional and local team across kingdom wide. SAS engineer needs to go to substation to solve the fault and restore the system in short time. The number of team member should not be large, it depends on two factors 1)number of systems and the size of geographical coverage area.

Intensive Development Program for engineers

National grid SA has started an intensive knowledge transfer program with all SAS vendors to develop its own SAS engineers/technician to be Experts, qualified enough and professionally certified. They will know how to master the automation system and maintain full administration of SAS. Those expert will be the key of success to run the remote maintenance center and provide the technical support for all maintenance engineers.

Pilot and experimental project

A conduction of pilot project in national grid SA premises is taking place these days to build virtual remote maintenance center by using Ethernet communication protocol. Three automation systems from different locations and similar SAS vendors will be connected to this center as first phase and all cyber security policy and recommendation will be applied. A weekly report will be internally generated to share the finding and output with all relevant divisions. The primary objective of this pilot project is to ensure that the risk from this transition is under control, determine the requirement of this installation and evaluate the use of remote access technology.

Budgeting

10 years ago, National grid SA. developed its own vision of smart grid transition and it made a huge investment on system upgrade. It included global upgrading program toward its own infrastructure, industrial control systems, and cyber security, which enhanced the capabilities and raised the possibilities to implement new systems and latest technologies. For these reasons, the cost of remote maintenance center installation will be a small additional phase of investment because the network readiness and strong base of foundation.

Fostering Collaboration with stakeholders

NG was aware that this transition could not be achieved by themselves alone. Collaboration between all vendors and national grid is a must. The best designs come from this collaboration by considering the National grid needs/ requirements and vendors capabilities. Number of meetings and workshops conducted to discuss the project and set the framework.

Estimated Return on investment (ROI)

The enormous benefits from Installing remote center, including cost savings, knowledge building and network reliability, which can be accomplished remotely as the following:

7.1 Tangible benefits

Operation technology system projects ROI should be based on tangible (or hard) benefits. Examples of tangible OT benefits (project savings / income) include:

60% reduction of travel expenses, remote support replacing on-site support, technician does not have to be on site or travel long distances in order to return the system to operation mode. downtimes are also reduced.

70% time saved eg increased productivity and reduction in time to complete tasks

Time saved eg from reduced length /number of SAS can be served at same time.

Time saved from reduced numbers of errors

Time saved from improving system reliability and having less maintenance or fewer problems to resolve

Time saved with improved software vendor support eg quicker responses, faster fixes

Reduced cost& time of System extension and retrofit projects.

50% fewer number of maintenance labor.

7.2 Intangible benefits

Intangible (or soft or non-financial) benefits should not be included within ROI calculations. Whilst they are often as important as tangible benefits, they are very difficult to financially quantify. Instead intangible benefits should be fully explained within the business case and where possible details given of any quantification or measurement. Examples of intangible OT benefits include:

Increased internal customer satisfaction (control, protection..)

Ability to offer improved remote service and support

Improved / automated business processes that the new system supports and enables

Faster and more accurate information.

Improved analytical solutions.

Better controls to improve data input accuracy.

Improved software vendor support and service, improved communications, better knowledge of software and system set up.

Ability to centralize Data archiving.

Ability for Cyber security control and network management

Better for risk management and disaster recovery.

	Locally	Remotely
Operational cost	Very high	60% reduced
Capital cost	Very high	65% reduced
Technical Experience	Fair	High
Operational efficiency	Good	Excellent
Policy &Standardization	Good	Excellent
Strategic project management	Difficult	Excellent tool
Smart grid & initiative	Fair	Strong base for SG
Cyber security control	Good	Good
Risk management	Good	Good

Table 3: compression between local and remote SAS maintenance

CONCLUSION

National Grid SA has set a global plan for smart Grid transition program. This program started years ago by collaborating with stakeholders in different domains, and then conducting several pilot projects to evaluate these experiments and determine the requirements for every phase in the projects. Next, by analyzing the output of the experiments and findings, corresponding recommendations are applied for the development, which are based on various international standards and recommended best practices, and are used as a basis for enhancing the administration of Substation Automation systems. All can use the guideline to develop the remote maintenance center characteristics of current and future products. NG has the motivation and determination to keep the circle of collaboration, evaluation, modification and implementation of smart grid transition. They acknowledge the fact that that circle played a critical role toward achieving their main objectives, and bringing ensures of business continuity.

References

Periodicals:

[1] IEC62351

[2] National Grid SA Smart Grid Envision (Nov 2013) By Abdulaziz A. Al-Sultan

[3] Model and frameworks for mastering complex system (third edition), Kevin Forsberg, Hal Mooz , Howard Cottermc.

[4] Introduction to remote control systems and remote maintenance systems for system monitoring, Eike Wedekind

[5] National Grid SA TES-P-107.05 Cybersecurity requirements for SAS

[6] Security Operation Center (SOC) in Utility Organization (SEP 2014), Babu Veerapa Srinivas