Kalkitech

Securing Power Distribution Assets from Cyber Attacks

White Paper

Preamble

Due to rapid growth of distributed energy generation, electrical distribution grid is evolving from unidirectional power flow network to bi-directional. Interwoven network topologies and rapid growth of renewable power generation units make the power flow indeterminant at a specific point of time. Utilities always want to operate the network smoothly, however there are huge pressure for them to keep the grid stable by tackling above challenges. Moreover, sever weather events and ageing network infrastructure make the situation worse. Abrupt change in generated power by the renewable generation points introduces constant stress to the infrastructure risking the failure. Distribution utilities do not have much visibility to the last mile of the grid even if they want to take any action.

Above challenge makes an electric distribution utility hard to operate and manage the network gracefully unlike previous era. There are various solutions available to overcome these challenges. However primary requirement for all those solutions is to provide connectivity with most of the distribution assets, network, and renewable generation plants directly to the utility control center for extensive visibility and control, Demand management, load balancing and planning, renewable generation prediction.

Advanced Low Voltage Monitoring & Control

Demand Response Management (DR)

Load Balancing and Substation Load profiling

Transformer Monitoring

Demand and Generation Prediction Analysis

Energy Storage Management

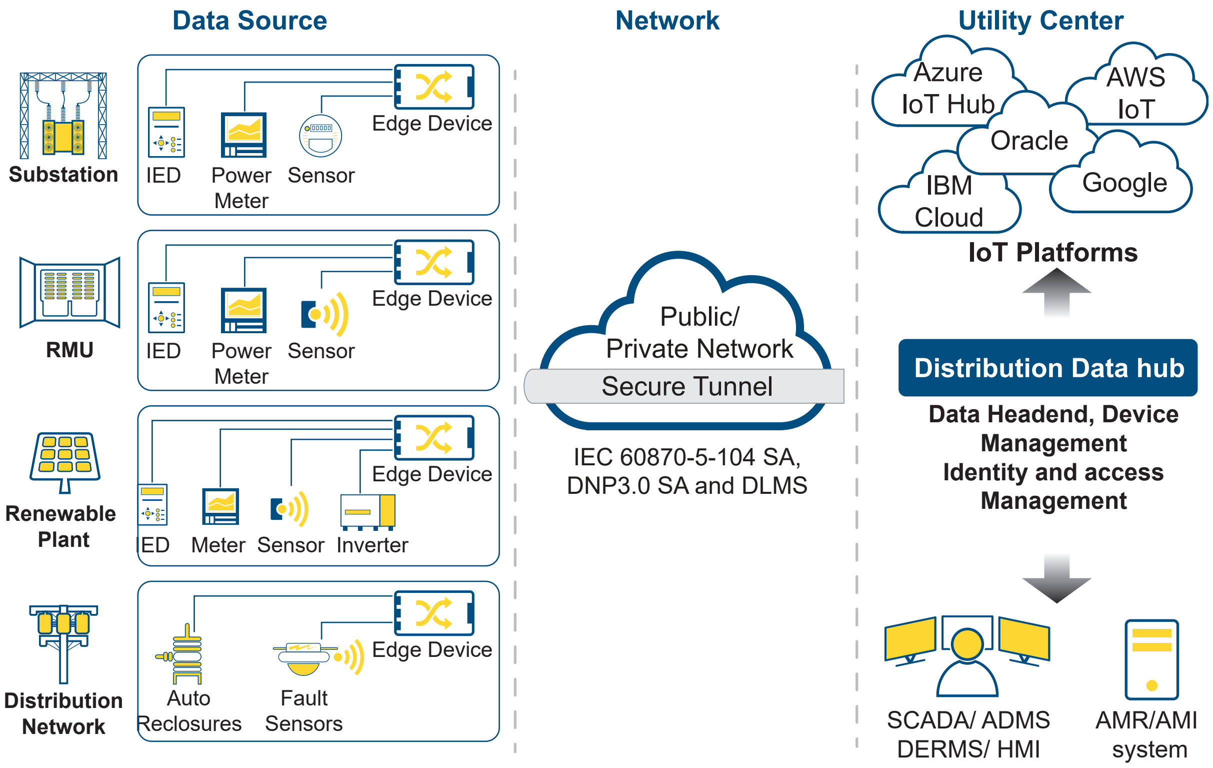
Advance Medium Voltage Monitoring and Control

Analytics using AI & Deep learning

Utility is deploying increased number of IoT sensors, and controllers directly on to the distribution network and equipment such as transformers, RMU, secondary substations, auto-reclosures and FPIs in the distribution grid at the same time extend direct connectivity with the renewable generation units or large-scale energy storage units. These new systems provide bi-directional communication with the control center or cloud and interact with other devices in the grid. With the adoption of distributed intelligent technologies that enable remote control and/or monitoring, more critical data are traversing through the communication networks necessitating stronger cyber-security.

Solution Architecture – Power Distribution Automation

Threats and vulnerability trends in the distribution grid and substation is increasing considerably due to several factors. In this paper we examine the unique aspects of cybersecurity in network and how can we architect a scalable and cost optimal solution without compromising the security. There are primarily three attack vectors for this kind of a system. **Edge device** or peripheral devices which connects field equipment/sensor/controllers with the communication network such as modem or gateway, **Network link** between field and the utility control center or cloud such as cellular network, and **utility control center** or software which collects data from field such as SCADA and AMR /AMI system.



To secure these critical points following criterial must be taken care at each level.

Edge Device at Field

Edge Device should minimally support.

1. Secure device management connectivity.
2. Role based device access.
3. Signed software/ configuration update.
4. Secure telemetry connectivity to share data with control center/ cloud.
5. Secure connectivity to field devices.

Edge devices deployed on the field should have **restricted access** for management and operation of the device. Any super user or root access to the devices should be provisioned only for local access. For remote access by system or security administrator should always require two-factor authentication to ensure that attackers cannot get into the system or devices, even if one of the authentication mechanisms is compromised. All passwords should be enforced as per strong password policy enforcement (eg: password length shall be at least of eight characters, the lesser of three or more different types of characters e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) and it should be rotated at a minimum, every 15 months. If any user has failed to login to the device after a defined maximum number of retry attempts, their account should be locked out for a specified period as defined by the asset owners.

As a **perimeter equipment**, edge device must have a built-in firewall. It should be possible for users to control the physical port as well as the logical port of the devices. It is an important defense tool which protects network assets from external attacks. Firewalls should be flexible enough to be configured for inbound and outbound traffic policies on each interface and local ports.

For any **control center connectivity**, device shall use x.509 certificate with bi-directional validation to establish a secure TLS1.3 connection. These certificates shall be authorized by a Certificate Authority (CA) with in utility scope. Hence edge device should have provision to install the private trust chain of the utility before setting up the device in the field. Edge devices should be pre-registered with the control center server. Device management and telemetry data sharing with control center shall always be through TLS 1.3 tunnel.

Each device and users are required to present authentication credentials and be verified by an authority to establish the trust before allowing connectivity to the system. Centrally deployed Identity and Access Management (IAM) systems based on Public Key Infrastructure (PKI) should act as authority for the authorization of an entity. It ensures that access to a utility system is granted only to authenticated users, groups, and software services. PKI cryptographic technique enables entities to securely communicate (encrypt communications using TLS), and reliably verify the identity of an entity via X.509 certificates with digital signatures. Standards for use of certificates within the utility industry includes IEC62351-8 (role-based access control) using attribute certificate or IETF RFC 6960 OCSP.

A digital signature can be used to validate the source and integrity of any information shared between entities. Firmware, configuration file and licenses are examples of the information which needs to be transferred to devices. Information should only be used if the signature appended in it is validated successfully.

All the new distribution and renewable assets shall be equipped with the RTU/Gateway meeting the above minimum requirements

Network

Network should minimally support.

1. Secure device management connectivity
2. Secure telemetry connectivity to share data with control center.

The communication network shall support TLS 1.3 and all communication shall be encrypted over a TLS 1.3 tunnel. All communication to the utility data collection system as well as device and identity management service shall be over TLS 1.3 to avoid man in the middle attack and data modification/spoofing.

Utility Control Center

Field interface and data collection software in utility control center should minimally support.

1. Secure data connectivity
2. Identity and access management services
3. Secure device management services

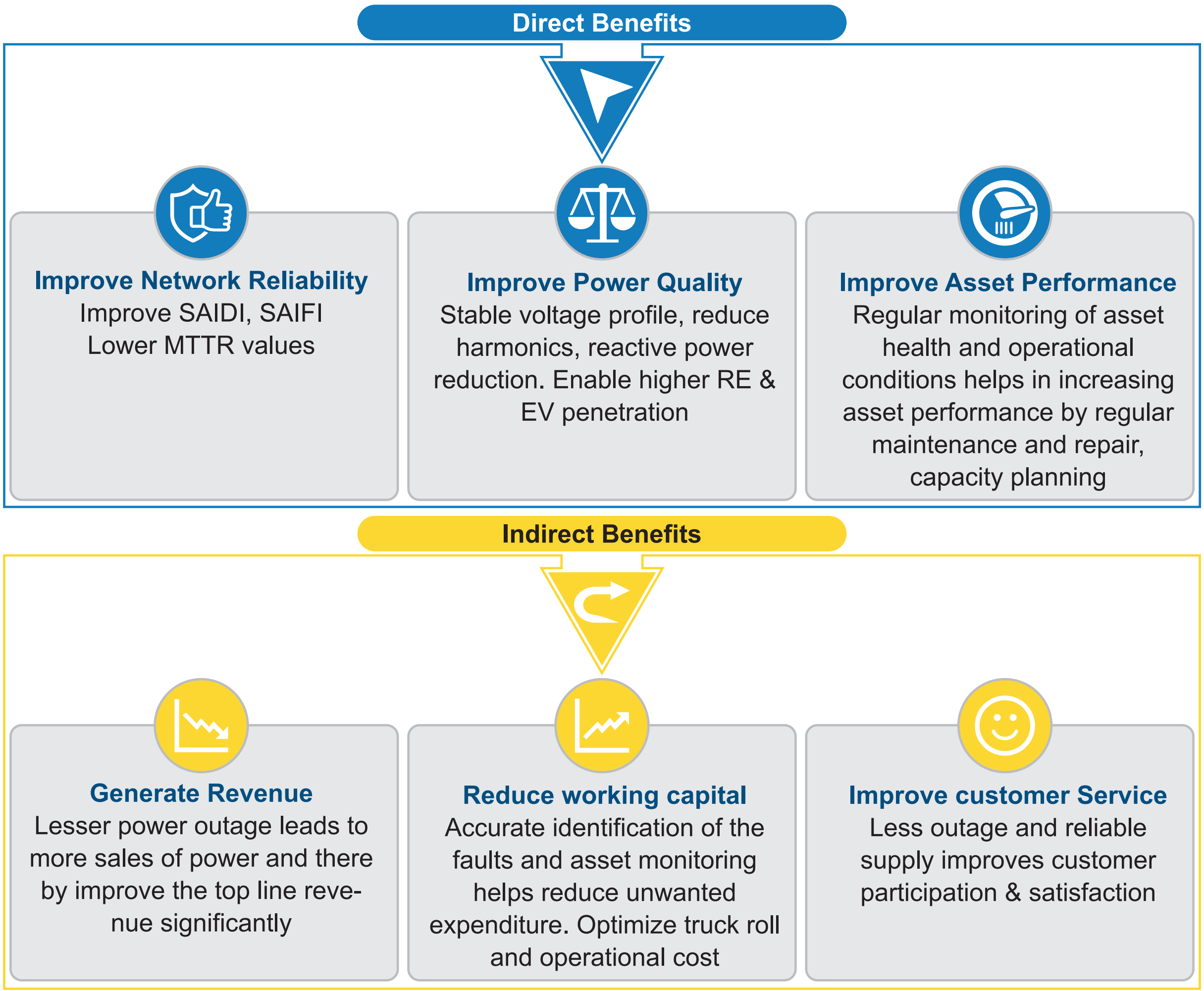
Field device data shall be able to collect securely collected at the control center. So, utility control center shall support secure termination of the field device connectivity. Software which are deployed in control center shall extend secure communication link for telecontrol.

Most of the existing Applications at control center like SCADA/ DMS or AMR/AMI system does not meet many of the present-day requirement of Security infrastructure, functional and system Resiliency and Scalability features. So, introducing **A distribution Data Hub** to handle all these functionalities in the Power distribution Architecture will be a good option.

Identity and asset management system as part of **Data hub** provide support to protect and secure the edge devices and thereby distribution grid assets from any un-authorized access. Identity and assess management service shall support **role-based access** control as per IEC62351-8 attribute certificate or IETF RFC 6960 OCSP. All **device management** support from the control center shall make use of identity and access management service. **Device Management** service in utility control center shall have access to firmware, documents, and configuration files with version tracking. Remote update of firmware, patches and license shall be possible using this service. Device management service shall also support notification support over mail or SMS in case of any critical events or alarms reported on the network or communication infrastructure.

Conclusion

Systems used in the distribution utility industry often have a life of at least 20 years. Therefore, it is critical to consider a security solution which can incorporate a strategy to protect legacy and newer devices, protocols, and software to meet the requirement of utility operators, regulatory bodies along with various new stakeholders including IT and cyber-security team.



Direct Benefits

Improve Network Reliability
Improve SAIDI, SAIFI
Lower MTTR values

Improve Power Quality
Stable voltage profile, reduce harmonics, reactive power reduction. Enable higher RE & EV penetration

Improve Asset Performance
Regular monitoring of asset health and operational conditions helps in increasing asset performance by regular maintenance and repair, capacity planning

Indirect Benefits

Generate Revenue
Lesser power outage leads to more sales of power and there by improve the top line revenue significantly

Reduce working capital
Accurate identification of the faults and asset monitoring helps reduce unwanted expenditure. Optimize truck roll and operational cost

Improve customer Service
Less outage and reliable supply improves customer participation & satisfaction

Corporate Headquarters: **Bangalore, India**
U.S. Headquarters: **Campbell, California**
Sales Office: **United Arab Emirates**

www.kalkitech.com
sales@kalkitech.com

Document: White paper
Version: 1.01.062021