Kalkitech

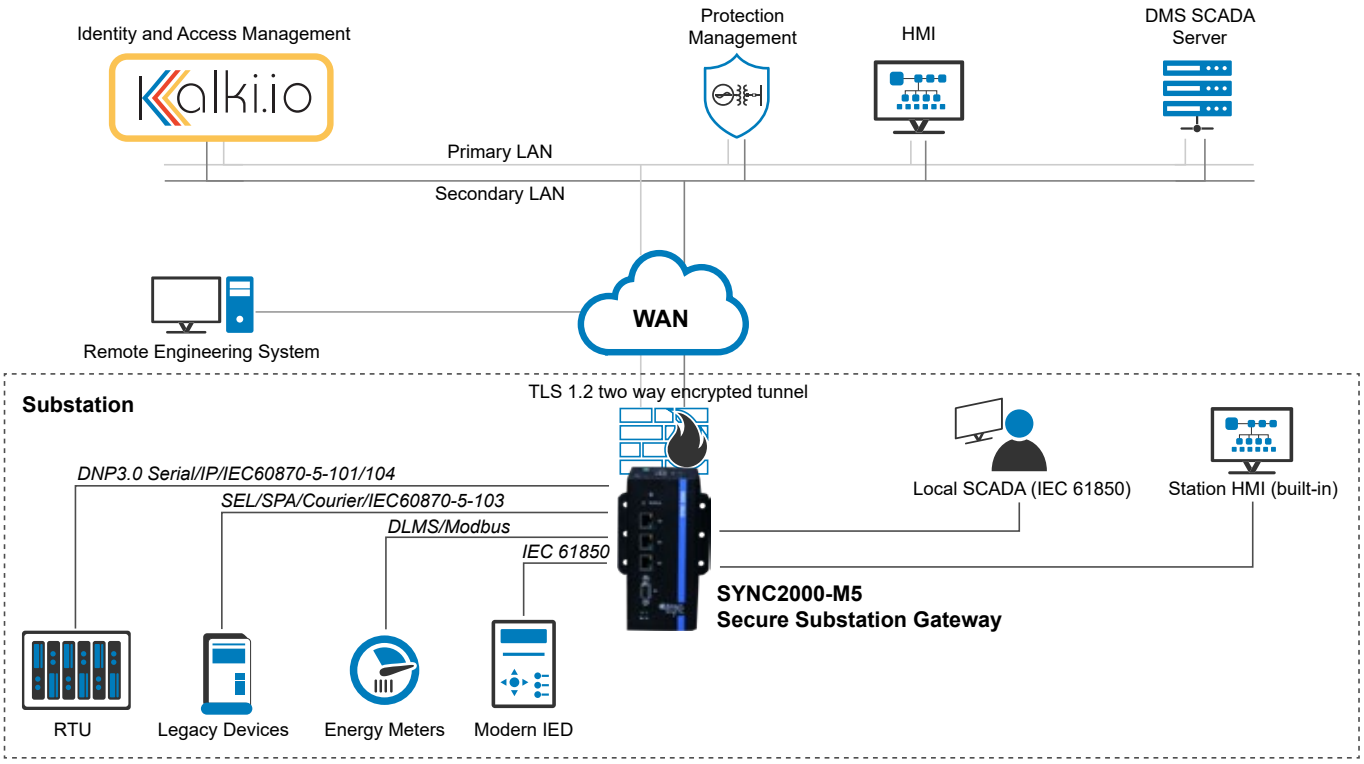
Secure Substation Gateway

With the deployment of more sophisticated automation system and equipment, utilities' priorities on the electrical grid system have been shifting to a focus on cybersecurity. State of the art automation standards rely on communication links at all levels in the system to exchange data. This requires communication of process level devices with bay level, between bay level devices, bay level devices and station level software, station level and control central level. As communication devices and links increase exponentially, so do the security threats and vulnerabilities in the system.

Today, hacking and cyber espionage are common occurrences across the world. Threats continue to increase in complexity and are targeted. Operation sabotage such as equipment and human safety failures, theft of power and usage data, vandalism, malicious software attacks and denial of service attacks are common threats experienced in substation automation systems today.

Substation gateways which are the access point or electronic security perimeter to the substation network are a critical asset and should incorporate a layer of security protection. An open standards-based, layered architecture is essential for utilities. Substation gateways should be highly available devices which ensure the confidentiality and integrity for engineering access and SCADA data conforming to NERC CIP critical infrastructure guidelines with real time access to key operations. They should defend against intrusions, man-in-the-middle and denial of service attacks as well as detect and log cybersecurity incidents and anomalies.

KALKITECH SECURE SUBSTATION AUTOMATION ARCHITECTURE



SYNC gateways and data concentrators deployed in utility substations can collect data from protection and metering devices. SYNC can connect and collect real time data, historical/profile data, fault file or event recordings on standard protocols such as IEC 61850, IEC 60870, DNP3.0 and Modbus, in addition to proprietary protocols from major Intelligent Electronic Device (IED) equipment vendors. Collected IED data can be stored, processed and converted to any telemetry protocol for transfer to the control center. This data can also be sent to a local SCADA station on IEC 61850 or a SYNC device can present the data over the built-in web HMI interface. In addition to data collection, SYNC devices can also be used to create a direct tunnel from a central protection management system to IEDs for remote configuration and parameterization. SYNC devices can be configured locally over a LAN or remotely over the WAN.

SYNC SECURITY FOR SUBSTATION AUTOMATION APPLICATIONS

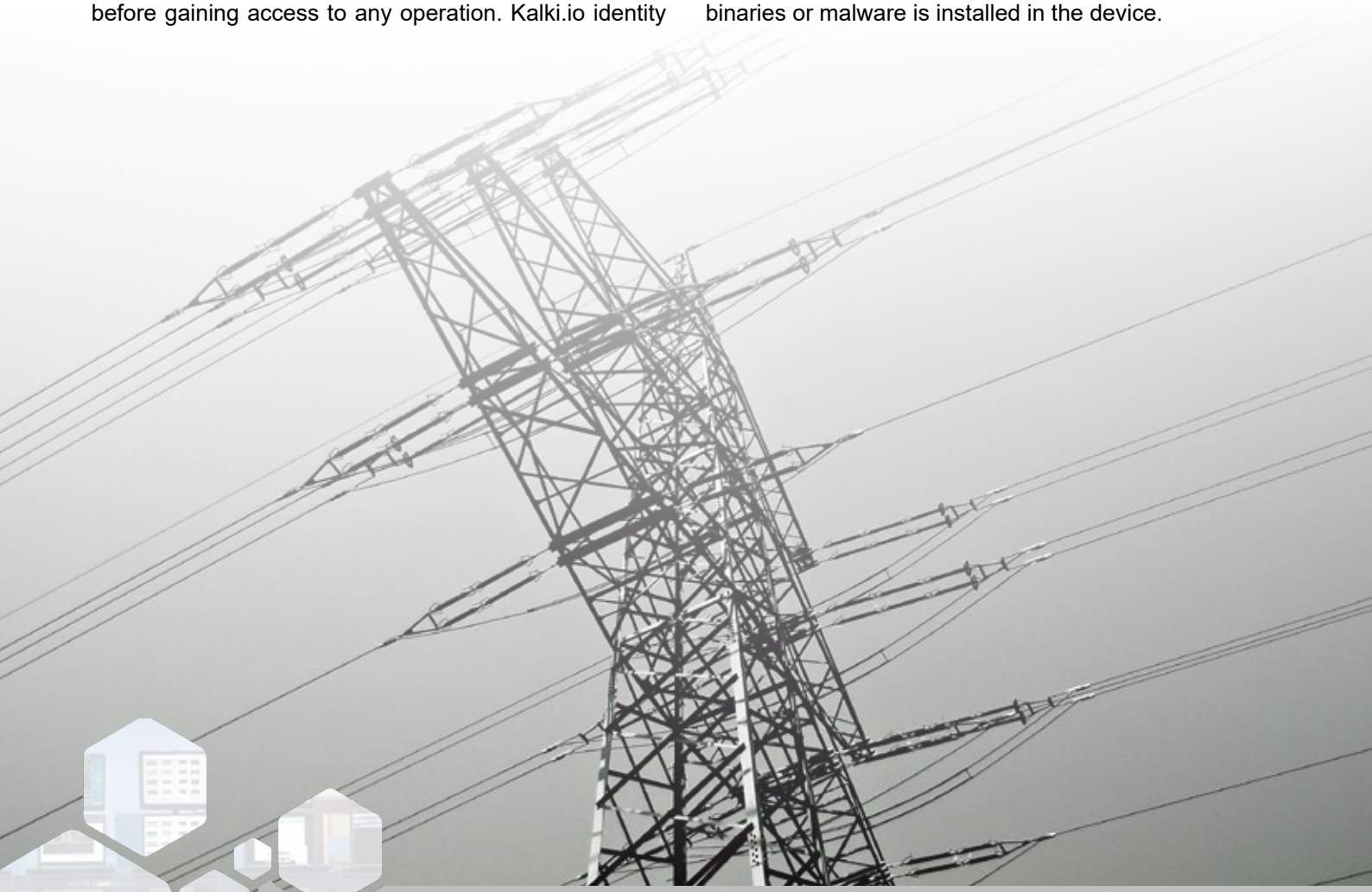
SYNC devices have a built-in firewall to control all the bidirectional network traffic from WAN to LAN at the substation perimeter. The user can configure physical ports as well as logical ports and is an important defense tool to protect network assets from external attacks. In addition, the firewall has the flexibility to be configured with inbound and outbound traffic policies for each interface.

SYNC gateways also help ensure confidentiality and integrity of data which its collected from field devices using various protocols. Data security is ensured by encrypting the data while in motion and at rest. Encryption reduces risk of man-in-the-middle, eavesdropping and replay attacks. Algorithms and protocols used for data encryption are compatible with industry standards for utility automation applications. The IEC 62351-3 standard defines the mechanism for implementing TLS-based security for all TCP-based communications used in utility networks. This is a generic standard which can be applied across all utility network protocols including DNP3.0, IEC 60870-5-104, Modbus, IEC 61850, etc. User authentication using challenge-response Secure Authentication (SA) as specified in IEC 62351-5, is supported in DNP3.0 protocol. Messages which need to be sent between substations as Routable GOOSE (R-GOOSE) are encrypted using an AES algorithm and authenticated using a secure hash algorithm (SHA V1) RFC2104. SYNC devices can connect with key distribution centers using Group Domain of Interpretation (GDOI) and collect the symmetric keys required for securely sending messages between substations.

SYNC also ensures that data is secure for all other associated services including network management, time synchronization, file transfer, and terminal access. The Network Management System (NMS) can access SYNC gateways only using Simple Network Management Protocol version3 (SNMPv3). Time synchronization of SYNC devices from station clock or synchronization of station devices by SYNC can be over Network Time Protocol version4 (NTPv4) or IEEE1588 which is a secure version of the protocol. Transfer of files/recordings such as event files, fault files from SYNC devices to the central server can use Secure File Transfer Protocol (SFTP).

SYNC devices use a X.509 PKI-based digital rights management system which is part of kalki.io Identity and access management. Kalki.io can be deployed on utility private network or hosted in a public domain. Digital rights management prevents spoofing, modification and nonrepudiation of device configuration and firmware. Role-Based Access Control (RBAC) provides fine grained permission settings to ensure specific operations are accessible only to authorized users or user groups. Any external actor must present authentication credentials, and be verified by kalki.io Certificate Authority (CA) before gaining access to any operation. Kalki.io identity and access management system can be configured to be operated in two modes i.e. per IEC 62351-8 RBAC using an attribute certificate for offline use or online use by permission validation of user using Online Certificate Status Protocol (OCSP) - IETF RFC 6960. Certificates are updated from CA using Simple Certificate Enrollment Protocol (SCEP) and validated using the keys received from the key distribution center using the Group Domain of Interpretation (GDIO) protocol. Configuration and management access can only take place over a secure IETF TLS 1.2 tunnel from either a local configuration utility EasyConnect or from kalki.io remote monitoring and identity and access management system. Web access for configuration and monitoring also uses a TLS1.2 tunnel created using a secure proxy deployed in the target PC.

All engineering data including configuration file, license file, settings can be transferred to a device only with a digital signature. Keys provided by kalki.io identity and access management system are used to sign all engineering data/files. Devices will accept firmware and patches signed by Kalkitech. Any other firmware is rejected by the device, ensuring that no unauthorized binaries or malware is installed in the device.



To monitor the user actions and security incidents, SYNC gateways use Syslog for logging. User access logs can track operations made to device settings and configuration. As per IEEE 1686 SYNC gateways also log events and alarms which can be monitored from an engineering tool, web HMI or from the remote management system - Kalki.io. These events and alarms can also be mapped to any telemetry protocols for users to monitor these from SCADA systems.

To ensure availability and resiliency against cyber threats SYNC device restrict access for management and operations. Remote access by system or security administrators require two-factor authentication to reduce the risk of attackers gaining access into the system or device. All passwords are enforced using a strong password policy per CIP-007-5 R5 (5.5) and are rotated based upon a configurable period. If any user fails successful login to the device after a defined maximum number of retry attempts, the user account will be locked out for a specified period as configured by the security administrator. SYNC devices provide only local console access to device administrator/root user and restrict complete remote access. SYNC gateways are tested and verified per the IEC 61850-3 standard to ensure that they cannot be tampered / vandalized using any attacks that compromise Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC).

RELATED PRODUCTS

Kalki.io Identity and Access Management System

SUPPORTED DEVICES

- SYNC 3000-M1, M2, M3, M12 (All models)
- SYNC 2000-M5