DATA LOGGER

Cyber Security & Communication Protocols

Overview

Schneider Electric provides end-to-end remote monitoring solutions consisting of a Data Logger data acquisition device, one or more sensors, wireless connectivity, and data and device management software. Schneider Electric's Data Logger device and software (IoT Platform) provide input for decision makers with continuous data on the state of their infrastructure and dispersed assets. The Schneider Electric solution is intended and engineered for passive monitoring and is not intended for control of critical assets and processes.

Fundamental cyber-security considerations for telemetry device manufacturers and service providers include encryption, authentication, remote device firmware update capabilities, and physical access restrictions. This document details the various, multi-layered cyber-security considerations of the end-to-end Schneider Electric offer, including at the hardware, wireless communication, data hosting, and data delivery layers of the technology stack.

Data Logger (Schneider Electric Industrial IoT Edge Device)

The Data Logger device is an ultra low-power, fully autonomous wireless telemetry device. The Data Logger collects data from a connected sensor(s) using industry-standard protocols, including analog (4-20mA and 0-10V), serial (RS485, RS232, and SDI-12), and discrete (pulse counting, digital I/O). Sensor data collection by the Data Logger occurs at configurable sampling frequencies.

The data obtained from the sensors is logged locally on the device with a timestamp and stored in industrial-grade internal memory in a proprietary binary format. This locally stored data is then transmitted to a Data Logger server (Schneider Electric Private Cloud or customer on-premises server) at a configurable transmission frequency or by exception for configurable thresholds.

Data Logger Communication Interfaces

All Data Logger devices are equipped with the following three communication interfaces:

1. Cellular Modem (4G, 3G, 2G)
2. Bluetooth Low-Energy for information on device status during installation and maintenance
3. USB for cabled console access and out-of-band configuration and trace-level debugging

Wireless Communication

Cellular Modem

The Data Logger communicates via cellular modem over industry-standard, encrypted, and secured protocols. Communication from the Data Logger to the server is in a binary, proprietary format. This communication is encapsulated in HTTPS or MQTTS using TLS 1.2, leveraging public-key cryptography as well as pre-shared keys (unique username and password) for MQTT device authentication. Secure communication from the Data Logger supports the following cipher suites:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256

The Data Logger uses dynamic, NAT'ed, and firewalled IP addresses offered by Schneider Electric's tier 1 cellular providers, which offer Verizon, AT&T, and T-Mobile network coverage in the US and coverage with several hundred other carriers around the globe via their own APNs.

There are no listening TCP/UDP communication ports to the Data Logger. More specifically, the device can initiate sessions with a server, but all incoming connections to the device are automatically rejected. Direct access to the Data Logger is theoretical rather than practical, as scanning Data Logger devices would first require penetrating the tier 1 cellular providers' firewalls and traversing NAT.

Communication sessions are limited in duration (typically 2 minutes or less) and allocated random IP addresses from a secured pool per session.

Security updates, firmware upgrades of the Data Logger device and embedded cellular modem* can be pushed through cellular communication only.

*Over-the-air security update capabilities of the modem are prerequisites that were demonstrated as part of the device certification and acceptance criteria by Verizon Wireless for access to the Verizon LTE network.

Bluetooth Low-Energy

Schneider Electric has developed multiple layers of security and authentication to enable a communication session with a Data Logger over Bluetooth via an embedded Bluetooth Low-Energy (BLE) module in the Data Logger and an iOS or Android device using the Schneider Electric mobile application. These layers of security and authentication include:

1. Pre-shared unique pairing key per Data Logger device
2. Communication encryption using Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) encryption

a. The first phase is key establishment, which is done through ECDH and HDKF. Salt exchange for each message is utilized to prevent reply attacks. The encryption is done with AES CBC, and data integrity is done using HMAC-SHA256.

b. This method provides the following benefits: eavesdropping on the connection does not reveal anything to the snooper, replay attacks are impossible, man-in-the-middle attacks do not reveal anything to the attacker.

3. Until the Schneider Electric mobile app, over BLE connection authentication is performed, the Data Logger does not answer any other messages. Moreover, in a case a non-authentication message (or a wrong authentication message) is sent, the Data Logger slams the connection. This is a general principle, related to all security aspects: both the Data Logger and the mobile app, in case an unexpected message with a bad data, not decrypted correctly, with a wrong length and etc. is received, the first side who is aware of the problem slams the connection.

USB Interface

It is important to note that sensitive information and operations are NOT available via the USB interface.

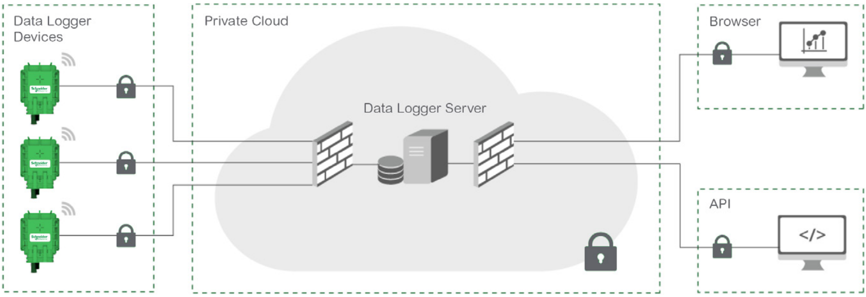
1. Firmware modification, upload, and download
2. Access or modification of stored data
3. Ability to upload any data to the server via the device

The USB interface is NOT physically exposed. It can only be accessed by removing a secured back cover plate of the Data Logger enclosure.

The USB interface has functionality that is limited to the following operations:

1. Provide trace output, which includes real-time information only (not historical information) that is limited in scope to operational and health status (e.g. battery voltage, device internal humidity, cellular signal strength, and health indicators)
2. Sending local Data Logger configuration commands and retrieving device diagnostics through Schneider Electric proprietary command language only that is protected from injections, such as changing the device APN, device reboot, and updating serial sensor communication parameters such as baud rate
3. Access to modem AT command interface for cellular troubleshooting

Schneider Electric Cloud Hosting



Data Packet and Routing Security

Data is transmitted by Data Loggers to the Schneider Electric Private Cloud services hosted on Amazon Web Services (AWS) in multiple, physically separated and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. All Schneider Electric services are built on fully redundant software stacks monitored and managed by a NOC 24/7/365. The redundant software stacks include the following security components:

- Stateful Packet Inspection (SPI) Firewall, which includes Advanced Threat Protection (ATP) at the L2 and L3 level
- Schneider Electric web application server, which authenticates and decrypts message payloads sent by the Data Loggers
- All servers have properly signed SSL certificates issued by a trusted certificate authority

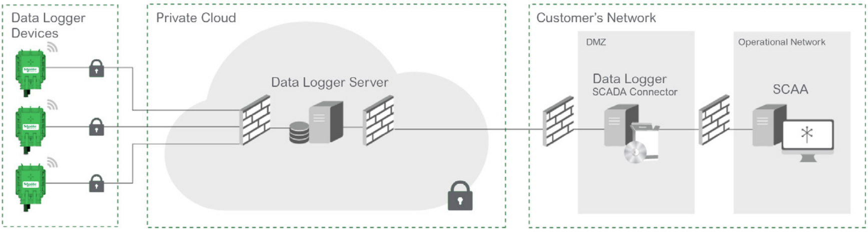
Data Storage Security

Schneider Electric utilizes data hosting provided by AWS in secured and redundant facilities. The services used by Schneider Electric include:

- S3 for configuration and binary archiving of transmitted payloads
- RDS for fully scalable and redundant database storage

For further information on S3 and RDS security and retention, please refer to AWS Whitepaper at the following link:
https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/awsoverview. pdf

API and Agents



Schneider Electric employs two industry-standard API methods (REST API and SOAP API) for data retrieval from the Schneider Electric Private Cloud. In addition, Schneider Electric provides three data retrieval Agents, which include DNP3, OPC-UA, and CSV, which are traditionally used for SCADA integration.

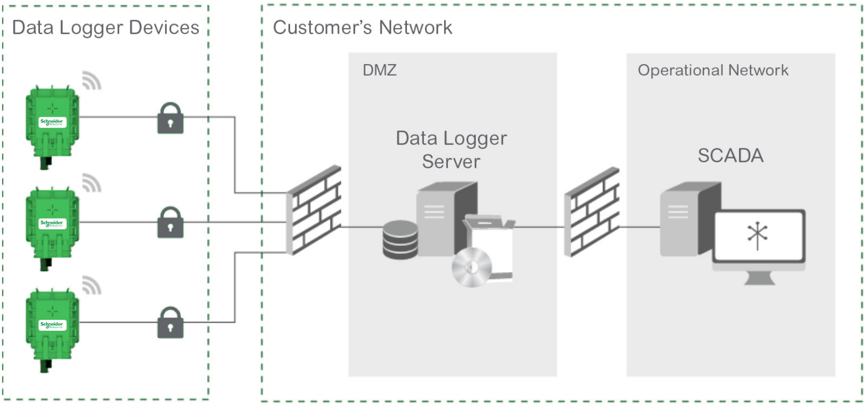
The SOAP API is being deprecated in favor of the more modern REST API implementation.

The REST API utilizes secure 64-bit OAuth 2.0 encoded security tokens, which can be revoked by the user who issues the token. Tokens enable software programs and Schneider Electric Agents to use nontransparent application authentication.

The APIs and Agents pull information via a single, secured HTTPS communication port utilizing TLS 1.2 (SSL) by initiating a session and polling at regular intervals as defined by the API and Agents' configuration scripts. The agents are limited with a maximum polling frequency to prevent an intentional or an unintentional Denial of Service attack. Schneider Electric Agents only use a single outbound TCP port over an encrypted connection to a specific host address, which enables simplified firewall administration and monitoring.

In the case of the DNP3 Agent, collected and cached data is pushed unsolicited via DNP3 protocol. In the case of the OPC-UA Agent, collected and cached data is presented to the services to the local LAN via a local OPC-UA server. In the case of the CSV Agent, collected and cached data is landed to named files in a designated directory and formatted according to the Agent's configuration files.

On-Premises Hosting



In the Schneider Electric On-Premises offering, customers can opt to host the application side on their own cloud services or local network. In this scenario, no information is stored by Schneider Electric and all Data Loggers are pointed to servers sitting on an IP address of the customer's choosing. All aforementioned application-level communication security is applicable to the Schneider Electric On-Premises offering. It is the responsibility of the customer to provide redundancy and packet-level security for any on-premises deployment.

Conclusion

This document is current as of August 29, 2019 and will be updated on an as-needed basis to reflect future enhancements of the Schneider Electric cyber-security and communication protocols.

For additional details, please contact:

David L. Kidd

Product Manager

davidl.kidd@se.com