LoopEdge IIoT Security

LoopEdge addresses security challenges in Industrial Internet of Things (IIoT) environments, as described in the following sections:

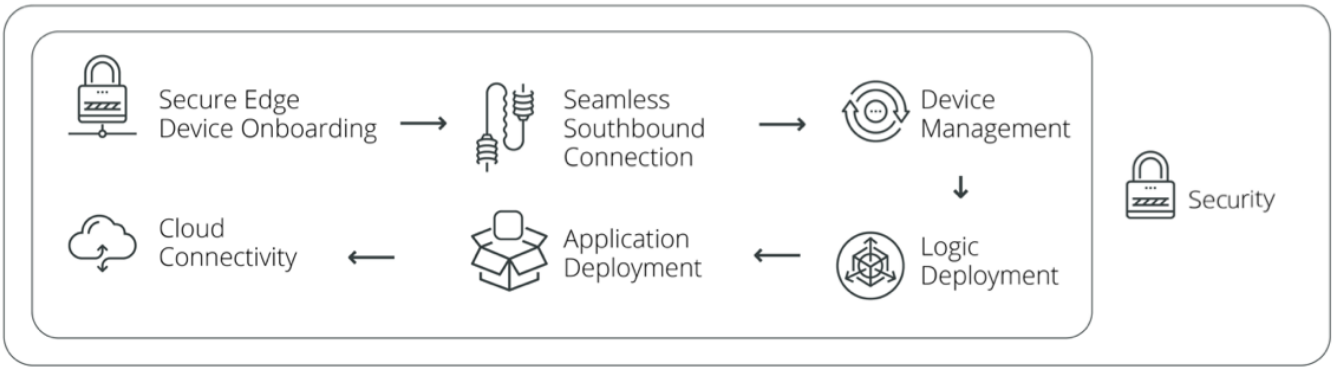
Security Challenges

In today's world of connected *things*, manufacturing enterprises face on-going security threats that can impact critical operations, resulting in costly downtime. With the trend of IoT data processing and analysis moving to *the edge* of the network, the need for endpoint and data transport protection has greater importance for devices that may be vulnerable to cyber attacks.

Above all, *security should be treated as a process*, not as a one-time task to check off a list. To that end, Litmus Automation continually assesses security recommendations and takes the necessary measures to keep the software in compliance with current standards.

Security Built into LoopEdge Architecture

Since its inception, LoopEdge software has incorporated strict security standards.



- **Secure Edge Device Onboarding** - See LoopEdge Deployment.
- **Seamless Southbound Connection** - LoopEdge uses the following standards for connectivity between the PLC and other devices:
  - ORiN (Open Resource Interface for the Network)
  - DOSA (Distributed-power Open Standards Alliance)
  - OPC UA (Open Platform Communications Unified Architecture)
  - MTConnect open standard
- **Device Management** - LoopEdge uses LwM2M (OMA) for device management.
- **Logic Deployment** - LoopEdge Flows enable data processing, with the ability to write application logic using Javascript and Python, including functions, as well as rules and alerts for event processing.
- **Application Deployment** - Users can create a private marketplace and deploy custom applications to run in a completely isolated, secure Docker environment within LoopEdge. It supports multi-tenancy.
- **Cloud Connectivity** - LoopEdge northbound device-to-cloud connectivity uses the following protocols. See Data Transport Security.
  - MQTT
  - HTTPS
  - LwM2M (OMA)

The LoopEdge framework addresses security in the following categories:

- Access Security: Allow only authorized personnel to access the device. Prevent at-the-device access to either credentials or data stored on the device.
- Data Transport Security: Protect data transferred to and from the device.

- Over-the-Air Updates: Ensure secure firmware updates.

Access Security

LoopEdge handles device access and threat detection in the following ways.

Passwords

- Only the most secure ciphers are used for password protection.
- Passwords must follow the rules defined in Password Requirements. Strong passwords provide the first line of defense against security breaches.
- Passwords are always stored in the system salted and hashed.
- Access to password hashes is restricted.
- LoopCloud can be configured with two-factor authentication, requiring an additional layer of authentication in order to access data sent to the cloud.

Remote Access via LoopCloud

LoopEdge works seamlessly with the LoopCloud platform for cloud-level processing and device management. Access LoopEdge devices from anywhere via the LoopCloud platform *Remote Access* feature, allowing flexible and secure access to your LoopEdge Devices for troubleshooting and configuration. See Remote Access to LoopEdge.

Data Transport Security

Data transmission occurs over an encrypted pipe, which uses SSL and TLS.

- All communication between a LoopEdge device and a user's browser is protected by transport layer encryption (SSL, TLS 1.3/1.2).
- The HTTPS protocol ensures secure access to LoopEdge devices.
- LoopEdge includes an SSL certificate from the Certificate Authority (CA) for each device. See also, Certificates.
- Additional certificates with private keys can be added to a device.
- LoopEdge DataHub includes a native and highly scalable message broker to publish data and subscribe to topics, with a high level of security and isolation, allowing multiple applications to consume data at the same time.

Over-the-Air Updates

All software updates, including the image files (.ova and .upd) updates, are digitally signed and encrypted. Data integrity and signature validity are verified before any upgrade.

Over-the-air (OTA) device firmware updates can be configured in LoopCloud using the following firmware features:

- **Distribution Sets**: Upload software module files to a device via the secure cloud connector.
- **Deployment**: Select multiple target devices for the update.