MYERS
EMERGENCY POWER SYSTEMS

WHITEPAPER

System Security and the IoT Inverter Connect Cloud Monitoring Solution

Prepared by Myers Emergency Power Systems

Background:

Myers EPS inverters are hardy, built to last, and require minimal attention and maintenance. However, as with almost anything in life, issues can always arise. The IoT (Internet of Things) Inverter Connect cloud monitoring solution for Myers EPS inverters allows remote monitoring of inverter telemetry (including voltages, currents, power levels, battery self-test results and alarm states) over the cloud to any device (smartphone, tablet, PC) with an Internet connection and web browser. Email and SMS notifications are also proactively sent out any time an issue is detected.

However, whenever infrastructure-grade devices – such as emergency power systems – are connected to the Internet, security concerns are legitimately raised, both for the guaranteed operation of the device itself, as well as the security of the other devices on the network. Some may also be concerned about the privacy of their inverter data.

Accordingly, Myers EPS has designed the IoT Inverter Connect solution from the ground up with device and network security as a **fundamental foundation**.

This white paper discusses the **multiple layers** of security that Myers EPS has designed into IoT Inverter Connect to ***eliminate*** any possibility of remotely impacting the potentially life-saving operation of the inverter, ***minimize*** the possibility of attacking other devices on the local network through the inverter, and ***maximize*** the privacy of their inverter data.

Unidirectional Data Flow:

The most fundamental security precaution designed into IoT Inverter Connect is that data flow between the inverter and its communication interface is only allowed to happen in one direction: from the inverter to the network interface. There is simply no physical channel for data or commands coming from the network to reach the inverter.

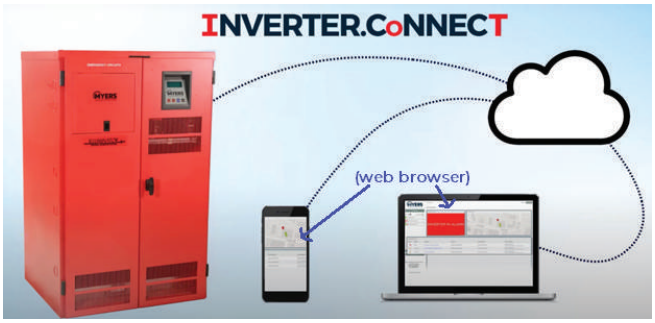
This is of course a compromise and limits the feature set of the solution. For example, you cannot remotely command the inverter to manually run its self-tests or remotely re-configure any of its parameters, because there is no physical channel through which to do so. This compromise was purposefully made, as we consider the security and reliability of our product to be paramount.

Unidirectional and Secure Cloud Connection:

Similarly, all data flows unilaterally, outbound, from the network interface to our trusted cloud servers. The network interface never accepts any inbound connections.

The outbound communications from inverter to cloud are encrypted using industry-grade **TLS 1.2 AES-256 encryption**. These communications implement the MQTT protocol, which uses HTTPS on port 443. In other words, they are as secure as your HTTPS connection to – for example - your online banking.

Finally, the fact that the network interface only communicates outbound and uses standard HTTPS on port 443 makes it ***much*** less likely that its connection to the cloud will be blocked by corporate firewalls, which obviates the (risky) need to add exceptions to the corporate firewall's exceptions list. Simply put, if you can Google stuff on a PC (this uses HTTPS) on a network, then IoT Inverter Connect can communicate with the cloud on that network, without ever contacting the IT department to mess with the firewall.



True Cloud:

When a user is using the IoT Inverter Connect cloud application, they are not communicating with the inverter. Rather, they are exclusively communicating with the cloud servers (which have buffered the telemetry from the inverter). This is the true definition of cloud, where your application logic and data are hosted securely on cutting edge cloud servers, not on end devices (which are always less secure or up to date). IoT Inverter Connect runs on **Amazon Web Services (AWS)**, which is considered one of the most secure, most reliable and most available (in terms of very low down-times) cloud hosting platforms. AWS servers are constantly being tested for security, and patched/upgraded when vulnerabilities are found.

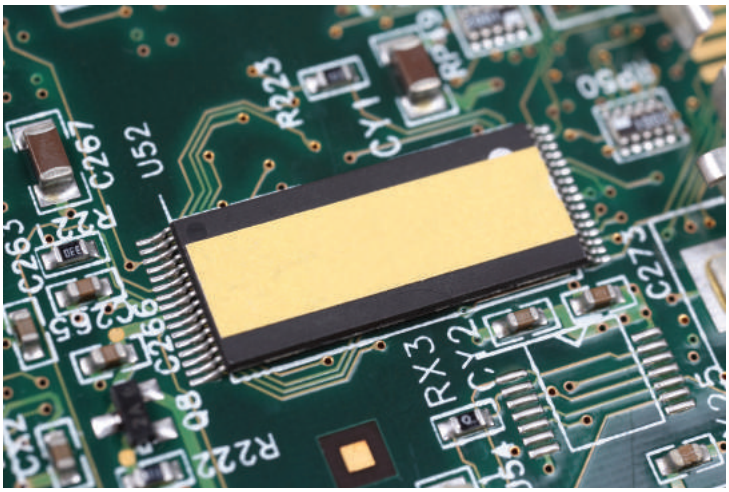
Communication between the cloud application and the web enabled devices that are used by customers to access it is secure **HTTPS** using the latest and greatest **TLS 1.3 encryption**. Inverter telemetry only lives on the cloud for 30 days, after which it is deleted, for privacy.

ProvenSec Certified:

The security of the IoT Inverter Connect network interface and the cloud platform is periodically audited and certified by **Provensec**. Provensec is a leading cyber security services provider specialized in network penetration testing. They subject the system to logical and technical application security attacks to test its resilience.

No Need for Firmware Update:

A system may be generally very secure, but if the firmware is updateable, a sophisticated malicious actor may find a way to put their own firmware on one or more end devices and compromise the system's security that way. Our inverters do not accept firmware updates from the cloud. Physical access is needed to firmware update, and all updateable components are placed inside the locked inverter cabinet.



Access Control:

The web application allows organizations to register multiple users, and securely share access to inverter telemetry and notifications amongst users. The following mechanisms were designed in to ensure the security of these features:

- User email addresses are **verified** in the registration process. For an email address to be granted permission to register, it must be on the whitelist. The only way to get on the **whitelist** is via verbal communication with Myers EPS, which involves customer verification steps.
- Passwords must meet **complexity criteria**
- As a fresh new user, you will at first have access to no inverters. There are two ways to add inverters to your IoT Inverter Connect web application account:
  - Add a new inverter. The pairing process to do so involves knowledge of the inverter's serial number, as well as pressing a button inside the inverter cabinet to complete the pair. This cannot be hacked remotely.
  - Have somebody who already has access to the inverter share it with your username.
- As a user with full 'read and write' access to an inverter, you may now share that inverter with other users, but:
  - The username that you share it to must be a registered and validated account
  - You can choose whether to grant 'read and write' permission to the person shared to, or more restrictive 'read-only' permission.

Conclusion:

By building a true cloud architecture, Myers EPS has designed the IoT Inverter Connect solution from the ground up with device and network security as a **fundamental foundation**.

This is accomplished via unidirectional data flow from inverter to cloud, secure encrypted outbound network connections from inverter to trusted cloud servers (with inbound connections forbidden), keeping the application data storage, processing and presentation on the cloud allowing for simplicity and high security on the inverter side (diminishing the need for firmware updates), using a secure, reliable and always up-to-date cloud provider (Amazon Web Services), using the latest and best encryption between the cloud and the web browsers used by end users, not allowing remote firmware update, and controlling access to the web application (via a whitelist) and inverters.