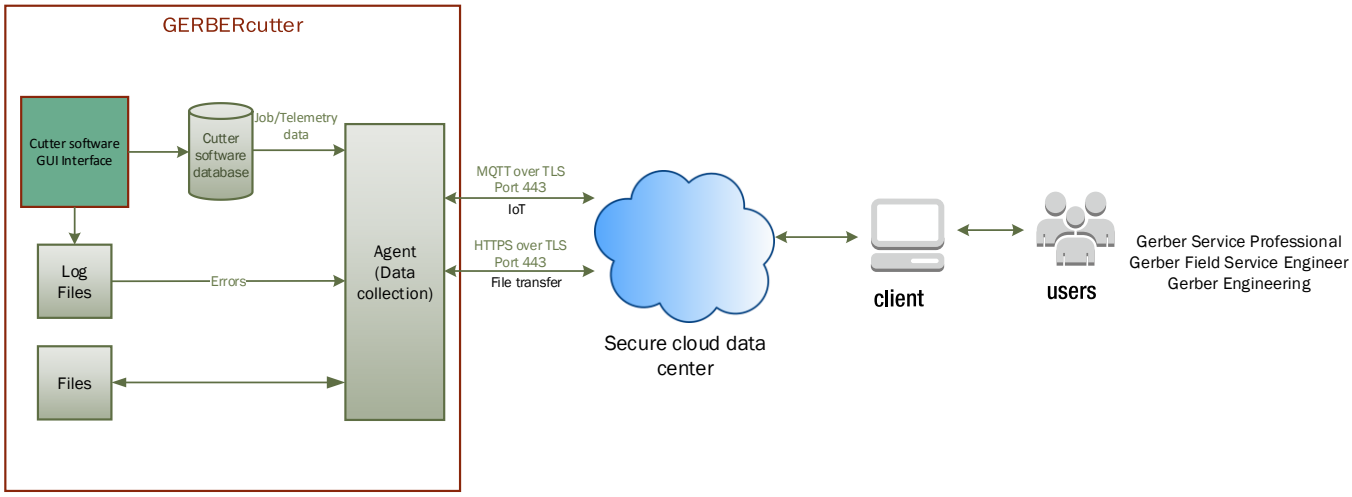
GERBER CONNECT Technical Note

Introduction

GERBERconnect embraces the growing trend of Internet of Things (IoT) to remotely monitor Gerber equipment. Some of the more important benefits include:

- Allows continuous visibility for Service and Engineering into the health status of systems with a high level of security.
- Allows monitoring customer equipment and assisting in remote diagnosis, resulting in quicker resolution of any reported issues.
- Ability to issue support requests directly from the machine to Gerber service for quick attention. Not available in the BETA release.
- Ability to remotely capture cutter image and cutter database backups for remote diagnosis.



High Level System Overview

Security

Gerber takes the security of customer data with the utmost of importance. All communications between the agent and the cloud take place over port 443 using a secure two-way authentication with X.509 certificates. For security reasons, all communications between the cutter agent and cloud initiate from the cutter. Communication with the agent cannot be initiated from an external source.

Data that is captured

A variety of information is collected by the agent that when combined together, provides a rich set of data to aid in the remote diagnosis of a customer problem. The primary categories of data include machine usage, telemetry, errors, and system information.

- **Machine usage** includes job start/stop times, time between jobs, idle time, error time, etc. Note that only usage metrics are captured and NOT cut geometry, i.e. customer intellectual property.

- **Telemetry data**. This is most prevalent on Paragon cutters due to the high number of sensors on the cutter. Some of the data collected includes motor and amplifier temperatures, motor and amplifier I2T values, amplifier bus voltages, motor currents during the homing sequence, circuit board voltages and temperatures, and servo hours of operation. Typically, telemetry data is collected once per minute only if it changes.

- **Errors** are collected by reading the cutter log files. Information gathered for each error includes the error message, error number and the level of severity ranging from 1 (most severe) to 5 (least severe).

- Miscellaneous **system information** is captured by making Windows WMI calls. Items of interest include product version numbers, Windows OS information, time zone names and hard drive capacity and free space. System information provides a quick reference to the exact configuration of the cutter system.

Remote Commands

Commands can be issued to the GERBERconnect agent that allow remote operations to be carried out on an as needed basis. Typical operations may include:

- Upload of cutter software log files to help diagnose problems
- Initiate and upload a cutter image backup to help diagnose a problem
- Send a configuration file to the cutter to restore a corrupt file
- Update the GERBERconnect agent

System Requirements

- The cutter computer must meet the following requirements
    - Microsoft Windows 7 (or newer) operating system
    - Have the software key and licensing software installed
    - Have Microsoft .Net Framework 4.5 (or higher) installed. Note, the install program will automatically download and install the correct framework but this will increase the install time
    - Non-interruptible internet access
- You must login with Administrator permissions to install this software, but administrator rights are NOT required for normal operation
- Arrange beforehand to have a company IT representative on standby in the event of firewall/anti-virus software issues

Firewall Considerations

Most installation problems relate to restrictions imposed by the customer's firewall. These generally can be resolved by working with the IT department by setting up a rule in the firewall software to allow the GERBERconnect agent (GCAgentService.exe) to get out through the firewall. All communications are initiated from the agent utilizing a secure two-way authentication using X.509 certificates. Communication with the agent cannot be initiated from an external source. The following parameters can be used as a guide to setting up communications on port 443.

- Set up as an outbound rule. The connection is established from the agent so an inbound rule is not required.
- Set the protocol type to TCP
- Set the remote port to 443
- Set the program executable to have access to: *"C:\Program Files (x86)\Gerber Technology\GERBERconnect Agent\GCAgentService.exe"*