BLUESKYTEC

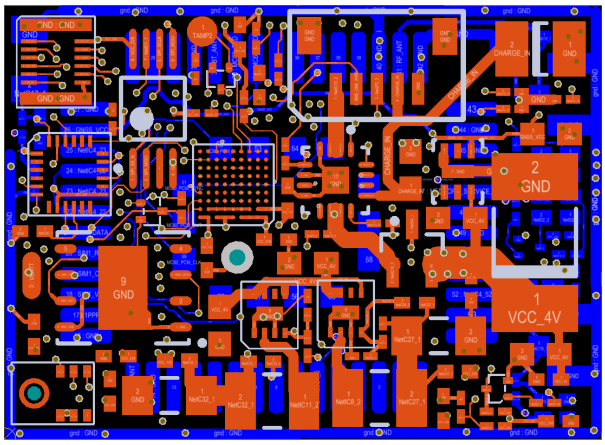
WWW.BLUESKYTEC.COM

M12pico Hardware-Hardened Security IoT Module

Available Q1, 2018

Overview

The M12pico is an ultra-miniature electronic module that integrates communications, cyber security and sensors into a single IoT device. There is a full suite of hardware-hardened security features for cyber security, including Trust Anchor, Secure Boot, Authentication and Encryption.



It has been designed to run from a standard Li-ion battery (e.g. model helicopter) for more than 48 hours, charged from a 5v USB power source. The module integrates sensors for GPS POSITION, MOVEMENT, VIBRATION, AUDIO and AMBIENT TEMPERATURE with GSM, GPRS and BLUETOOTH communications.

Description

M12pico is a member of the Blueskytec M12 family of hardware-hardened security IoT modules. M12pico integrates a Flash Based FPGA, memory, interfaces, communications and sensors onto a micro-miniature 8 layer, 21x29mm circuit board. The circuit board contains everything the system needs to run as a hardware-hardened security IoT processor connected to the internet via the integrated GSM/GPRS/BT module. The only external components required are the GSM antenna, GPS antenna and Li-ion battery. A typical 1200mAh model helicopter battery will last for 96 hours using the advanced energy saving modes, and can last for weeks in a dormant state waiting for an alert (vibration etc).

Cyber security architecture

The active processing element used on M12pico is the Lattice MachXO3-4300 device. This is an instant-on FPGA and is freely available for an OEM to design and develop their hardware code.

For OEM customers wanting to take full advantage of the Blueskytec cyber security IP we have a VHDL library that can be used to provide hardware trust anchor, key management, trusted boot, encryption & decryption services, and tamper detection. This patent-pending technology uses approximately 4000 elements of the device, which occupies 90% of the available space.

User/BST program development

A 16 bit processor is available for users to program and provide the communication engine to the MC60. Blueskytec have a standard software library for driving the MC60 GPRS, SMS and USSD interfaces.

BLUESKYTEC LTD, 24 BARTON STREET, BATH, BA1 1HG
COMPANY REGISTERED IN ENGLAND AND WALES
NUMBER 7958649 VAT No 132160265

To develop code and program the unit (either by Blueskytec or the OEM) the module is inserted into the JTAG development system. This routes the JTAG to a standard 14 pin header so that the Lattice programming interface can be attached. The key fill port (9K6UART) is routed to a 9 way D type. Led's are available for testing. Blueskytec has a range of IP both software and VHDL hardware that can be programmed into the unit.

Applications

Blueskytec has teamed with a number of worldwide partners to leverage this technology into consumer products. Applications include:- Tracking of autonomous personal vehicles, smart sensors, marine applications, industrial monitoring and general tracking, monitoring and control applications.

M12pico Specifications (TBC)

- Hardware Hardened Security IoT Module
- 21mm x 29mm x 5mm.
- 5V DC, 500mA standard USB wall charger input
- Connection for a 3.7v Li-ion battery, supporting charging up 2.4Ah Capacity.
- GSM/GPRS world-wide connection with SMS and Data.
- 21.4 kbps download, 21.4 kbps upload, GPRS data – class 1 (1 rx + 1 tx timeslots)
- 85.6 kbps download, 21.4 kbps upload, GPRS data – class 8 (4 rx + 1 tx timeslots)
- 64.2 kbps download, 42.8 kbps upload, GPRS data - class 10 (3 rx + 2 tx timeslots)
- Bluetooth interface with integrated antenna.
- GPS with battery backup and instant acquire.
- Accelerometer for vibration and movement monitoring.
- Microphone for sound recording.
- Expansion header (for programming, external sensors, external comms, external control).
- GSM and GPS sockets for off-board antenna.
- Hardware hardened security architecture with 256 bit key per board, Anti-tamper, Secure boot, Trust Anchor, Key Fill port, One Time Pad, authentication and encryption using BST256.
- Lattice MachXO3-4300 FPGA, 11kByte SRAM, 32kByte FLASH,
- External 128kByte battery backed SRAM.
- Available on header, JTAG, power, 2 x digital I/O (I2C) + 1 UART
- No ITAR or Dual use restrictions

Client Side Software

WWW.BLUESKYTEC.COM

How does a customer manage the high volume of data generated by a large number of deployed M12's? Blueskytec has a proven answer to this that can integrate with a clients existing tracking system or be standalone.

Blueskytec works with the OEM and their customer to provide a secure, robust and user-friendly software system to manage the installed base of M12's. With many 1000's of units potentially connecting to the cloud with information, an automated system must be used to manage the large volume of data. This is how Blueskytec helps the OEM and their customer deliver an integrated solution.

The system solution consists of 4 items: M12's, connectivity via a service provider (WiFi, GSM, Satellite), OEM Server, Client Access.

Connectivity: M12's connect to the World Wide Web thought the use of any interface available. On the M12's, the GPRS Air Interface is used. This Air Interface is standard GPRS with an embedded SIM on the unit. This SIM can be supplied by us using our Emnify global partner, or can be supplied by the OEM's telecommunications partner (Vodafone, Telefonica/O2, EE etc). The SIM is locked with a PIN to the unit and cannot be removed. If it is, the SIM is locked using the standard PIN services. If the unit is probed whist operating the unit will enter tamper alarm and stop working, thus no information can be gained from side channel analysis of the unit. The Telecommunications provider route the SMS and GPRS data through their network to the OEM server. This data can be FULLY ENCRYPTED so the Telecommunications provider cannot access the information.

OEM Server: The OEM server is an SQL database and Apachie Server system that accepts HTTP POST JSON FORMAT GPRS data messages from all M12's. It also generates messages to the M12's for control. It also accepts SMS text messages (when GPRS is not available), passes these and populates the database correctly. This OEM server will be located at the OEM facility or chosen secure location. All data in the database can be encrypted and no part of the Server has access to unencrypted data.

Client Access: The client application (web browser, PC/MAC application, smart phone app etc) access the OEM data base with requests for data. This data is returned to the clients application and displayed.

End-to-end security: For complete end-to-end security Blueskytec can supply a hardware "Dongle" that decodes and authenticates the data from the M12's. Without this attached to the users access device the data is useless. The Dongle attaches to the users device via Bluetooth.

Please contact us for a demonstration of the system.