AN2699

UART Bootloader for SAM L10/SAM L11

Introduction

Many modern embedded systems require application image updates to fix errors or support new features. A small piece of code can be added to the main application to provide the ability to download updates, replacing the old firmware of the device. This code is often called a Bootloader, as its role is to load a new program at boot. A Bootloader always resides in the memory to make it possible for the device to be upgraded at any time. Therefore, it must be as small as possible.

This document describes the design and operation of a UART Bootloader developed for the SAM L10 and SAM L11 devices.

Table of Contents

1. Features

The following are features of the UART Bootloader:

- Small size (1 KByte)
- Uses UART Rx and Tx pins, and the Bootloader Entry pin
- Running out of SRAM allows self updating
- Simultaneous writing to Flash and next Buffer Reception to speed up the update process
- Optional image verification using the CRC32
- Source code is available, which can be customized to user requirements.

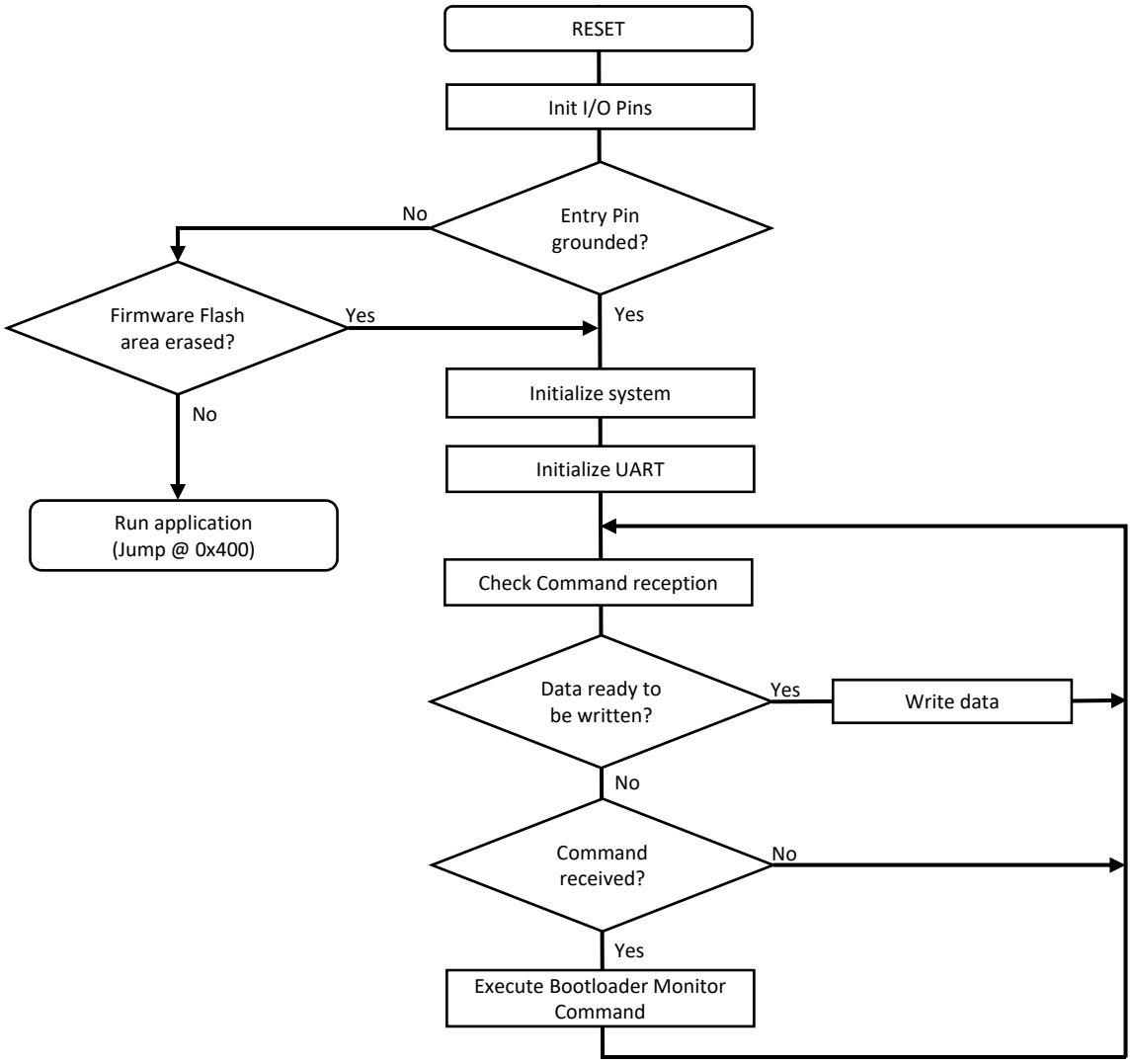
2. Bootloader Implementation

2.1 Bootloader Flow

The startup sequence of the Bootloader is as follows:

- Initialization:
  - I/O pins initialization
- Entry methods condition check:
  - Cache is disabled
  - Wait States = 2
  - Performance Level = 2
  - 16 MHz clock
  - UART initialization
- Bootloader Monitor execution (if one entry method is verified)

Figure 2-1. UART Bootloader Flowchart

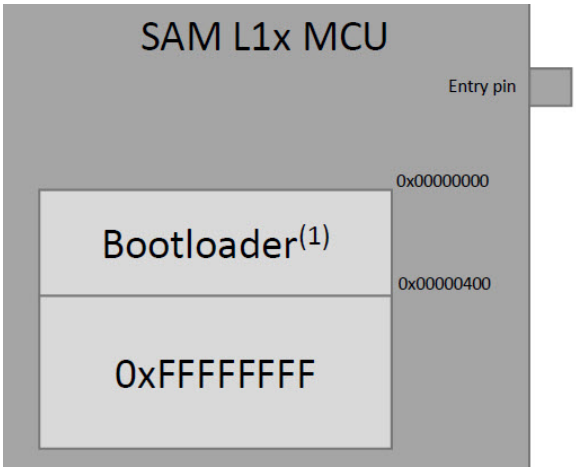


2.2 Method of Entry

Once the Bootloader is flashed into the device, the Bootloader monitor can be entered in two different ways:

1. The Bootloader monitor will run automatically if there is no valid firmware in the application Flash memory region. The firmware is considered valid if the first word is not 0xFFFFFFFF. Normally, this word contains an initial stack pointer value, therefore the first word will never be 0xFFFFFFFF unless the device is erased.

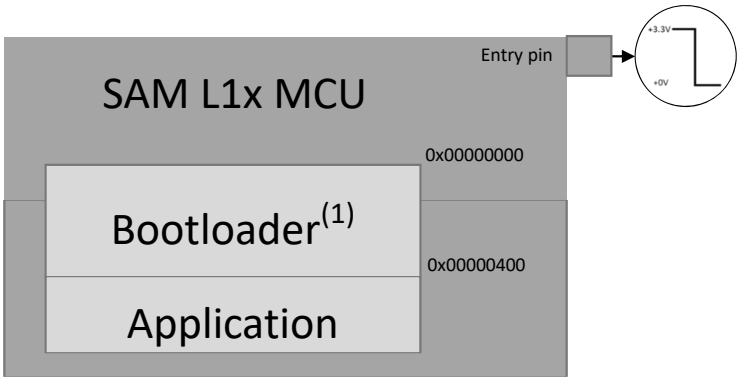
   Figure 2-2. First Bootloader Entry Method



   Note: 1. Bootloader runs in the Secure world for SAM L11 devices.

2. The Bootloader commands monitor will run on an external request if the value of the Bootloader Entry pin is low when the Bootloader execution starts. The Entry pin takes priority over any other method of entry.

   Figure 2-3. Second Bootloader Entry Method



   Note: 1. Bootloader runs in the Secure world for SAM L11 devices.

2.3 Hardware Configuration

The UART pins used by the Bootloader depend on the type of device, which are listed in the following table.

Table 2-1. Hardware Configuration

Device	UART Tx	UART Rx	Entry Pin
SAM L10	PA16	PA17	PA19
SAM L11	PA16	PA17	PA19

The Bootloader Entry pin has an active low level. The value of the pin is sampled at the beginning of the Bootloader execution. Although the internal pull-up resistor is enabled before sampling the pin, it is recommended that the Bootloader Entry pin be pulled up externally for improved noise immunity.

The UART setting used by the bootloader is 115200 8,N,1.

Note: These are the default settings used by the Bootloader, but it can be modified by the user as desired for more flexibility.

2.4 Device Configuration (SAM L11 Only)

The RXN User Row fuse bit (RAM is eXecute Never) must be cleared or the SAM L11 will not be able to enter Bootloader mode, as the Bootloader runs from the RAM to allow for self-update.

3. Bootloader Monitor Commands

All Bootloader commands have the same general format, as shown in the following table.

Table 3-1. Bootloader Commands

Command ID	Guard Value	Data 0	...	Data N
1 byte	4 bytes	4 bytes	...	4 bytes

The number and meaning of the data words varies with the command. All data must be sent in a little-endian (LSB first) format.

The *Guard Value* must be a constant value of 0x2b620bc3, which provides additional protection against spurious commands.

All bytes of the command frame must be sent within 100 ms of each other. After 100 ms of idle time, an incomplete command is discarded and the Bootloader returns to waiting for a new Command ID. This behavior allows the host to re-synchronize in case of synchronization loss.

The Bootloader understands the following commands:

1. `Unlock (0xA0).`
2. `Data (0xA1).`
3. `Verify (0xA2).`
4. `Reset (0xA3).`

The `Unlock` command must be issued before the first `Data` command and has the following payload:

- Data 0 – Starting Offset
- Data 1 – Image Size

The Starting Offset is the offset from the beginning of the Flash memory. To upgrade the Bootloader, this value must be set to zero.

The application image offset is device-dependent, and valid values are listed in the following table. The image offset must be aligned at an Erase Unit Size boundary, which is also device-dependent. The image size must be in increments of Erase Unit bytes.

Table 3-2. Valid Values for Application Image Offset

Device	Application Offset, bytes	Erase Unit Size, bytes
SAM L10	1024	256
SAM L11	1024	256

The `Data` command is used to send image data and has the following payload:

- `Data 0` – Starting Offset
- `Data 1 – Data N` – Image Data (Erase Unit Size bytes)

A starting offset must be located inside the region previously unlocked through the `Unlock` command. Any attempts to request the write outside of the unlocked region will result in an error, and the supplied data will be discarded.

This Bootloader supports simultaneous Flash memory write and reception of the next block of data. The next block of data may be transmitted as soon as the status code is returned for the first one.

Due to this behavior, the status code for the last block will be sent before this block is written into the Flash memory. To ensure that this block is written, the host must send another command and wait for the response. Therefore, the `Verify` or `Reset` command must be sent after the last block of data.

In case the `Verify` command is used, and actual verification is not required, the fields of the `Verify` command must be set to include at least one block of Erase Unit Size bytes, and Image CRC can be set to 0. In that case a CRC Fail status will be reported, which may be safely ignored.

The `Verify` command is used to verify the image data and has the following payload:

- Data 0 – Expected CRC32

Image CRC is a standard IEEE CRC32 with a polynomial of 0xEDB88320.

Internal CRC is calculated based on the values read from the Flash memory after programming, so it verifies the whole chain. Image CRC is calculated over the previously unlocked region.

The `Reset` command is used to exit the Bootloader and run the application, except when the Bootloader entry is done using the Bootloader entry pin. In this case, the entry pin value must be set high once the programming is done and a hardware reset must be performed to run the application.

The `Reset` command has the following payload:

- `Data 0` – Arbitrary Value 0
- `Data 1` – Arbitrary Value 1
- `Data 2` – Arbitrary Value 2
- `Data 3` – Arbitrary Value 3

The supplied arbitrary values are passed to the application in the first four locations in the SRAM.

4. Bootloader Monitor Response Codes

The Bootloader will send a single character response code in response to each command. Sequential commands can only be sent after the response code is received for a previous command, or after a 100 ms time-out without a response.

The following are possible response codes:

- OK (0x50) – Command received and processed successfully
- ERROR (0x51) – There were errors during the processing of the command
- INVALID (0x52) – Invalid command is received
- CRC_OK (0x53) – CRC verification is successful
- CRC_FAIL (0x54) – CRC verification failed

5. Programming Algorithm

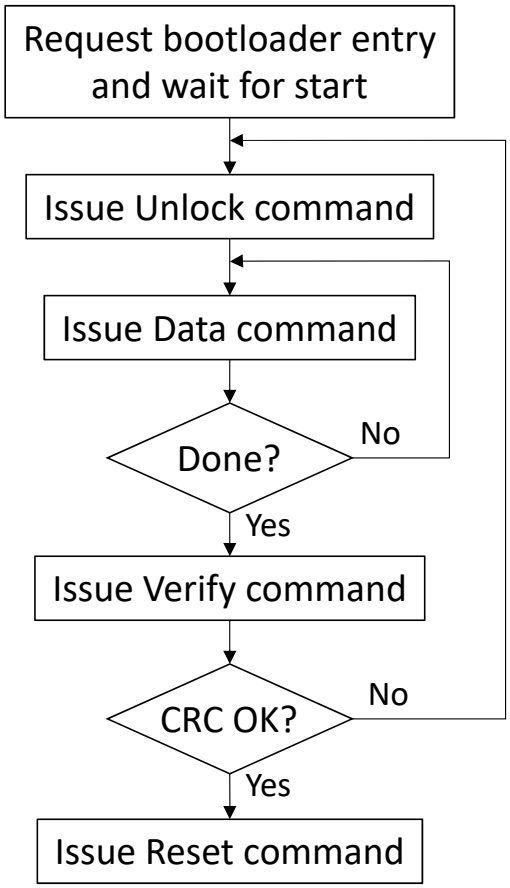
After issuing each command, the host must wait for the response code for at least 100 ms. If no response code is received during this time, the command may be considered lost and may be repeated again.

The host controller must perform the following actions to update the firmware:

1. Request the bootloader entry.
2. Wait for at least 5 ms for the bootloader to start.
3. Issue the `Unlock` command with the required image parameters.
4. Send the `Data` command with the application data.
5. Application data is programmed. Repeat item 4 until the entire image is written.
6. Issue the `Verify` command, and check the response code.
7. If a valid CRC was supplied in the `Verify` command, but the response code is not CRC_OK, then repeat the update starting from step 3.
8. Issue the `Reset` command.

This algorithm is illustrated in the following figure.

Figure 5-1. Programming Algorithm



6. PC Utilities for Working with the Bootloader

6.1 Software Requirements

Python 2.X is required to execute the provided scripts. The latest version of the Python 2.X is available for download from the following location: https://www.python.org/downloads/.

Note: In addition to Python, the pySerial module is required to access the computer's serial COM port. The latest 2.X version is available for download at https://pypi.org/project/pyserial/.

6.2 Boot.py Utility

The update utility, `boot.py`, takes an image and uploads it over the serial port, and it has the following syntax:

Options:

```
-h, --help            show this help message and exit
-v, --verbose            enable verbose output
-i PATH, --interface=PATH    communication interface
-f FILE, --file=FILE         binary file to program
-o OFFS, --offset=OFFS       destination offset (default 0x400)
-r,      --reboot               send the reboot command
--boot                 enable write to the bootloader area
```

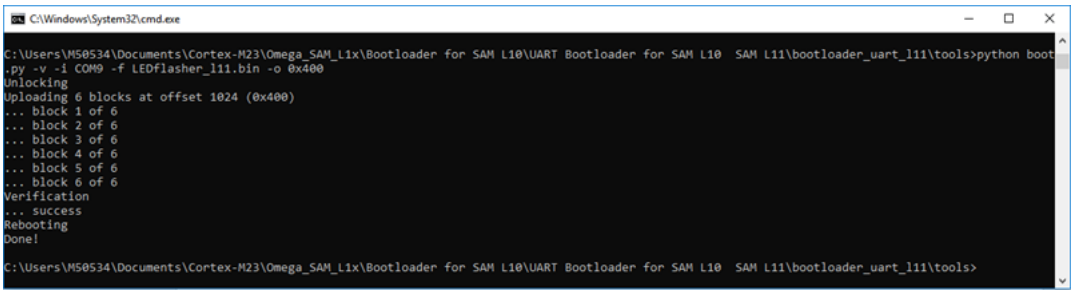
Example invocation:

```
boot.py -v -i COM12 -f test_app_l10.bin -o 0x400
boot.py -v -i COM12 -r
```

The Bootloader size is 1 kB long, so the application must be linked at 0x400 offset.

The `--boot` option is necessary if the image has an offset less than the Bootloader size. This is an additional protection to prevent accidental overwrite of the Bootloader area.

Figure 6-1. Successful Programming of an Application Linked at 0x400



6.3 Troubleshooting Guide

6.3.1 Verify Python Version

It may happen that the boot.py call leads to an error message.

Ensure that the Python 2.X path is defined in the environment variables after installation, and is used instead of Python 3.X even if version 3.X is already installed on the host, otherwise boot.py cannot be called by the python sequence.

6.3.2 Check Bootloader Execution with Terminal

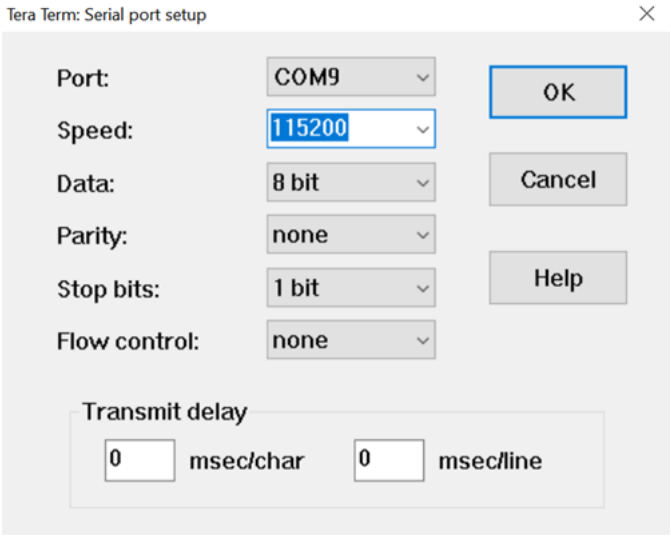
There might be a situation, the host does not receive any response from the Bootloader, see figure below:

Figure 6-2. No Response from Bootloader

```
C:\Users\M50534\Documents\Cortex-M23\Omega_SAM_L1x\Bootloader for SAM L10\UART Bootloader for SAM L10  SAM L11\bootloade
r_uart_l10\tools>python boot.py -v -i COM9 -f LEDflasher.bin -o 0x400
Unlocking
Warning: no response received, retrying 1
Warning: no response received, retrying 2
Warning: no response received, retrying 3
Error: no response received, giving up
```

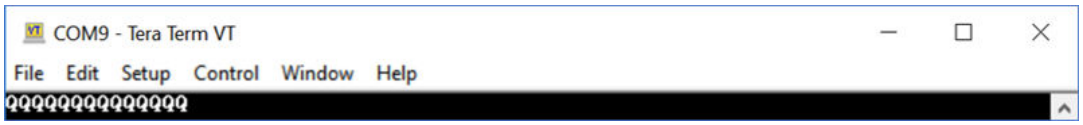
In that case, a terminal can be used to verify whether the Bootloader is running on the device or not, for that users need to use the following COM-port settings:

Figure 6-3. Bootloader COM-Port Settings



If the Bootloader is running, “Q” characters must appear when typing any character on the terminal:

Figure 6-4. Bootloader Response Through Terminal



Note: The terminal must be connected to the COM port dedicated to the UART pins.

If not, verify the following points:

- If there is already a valid firmware in the Flash memory, ensure the Bootloader entry pin is grounded, then reset the board
- For the SAM L11 device, check that the UROW RXN fuse bit is cleared

7. Revision History

Revision A - May 2018
Initial release of this document.

Revision B - February 2019

Section	Updates
Introduction	New introduction text added.
Features	Minor editorial updates and removed typographical errors.
Bootloader Implementation	• Updated Bootloader Flow with a new Block Diagram • Updated Method of Entry with new Bootloader diagrams • Updated Hardware Configuration with a new table and corrected typographical errors. • Updated Device Configuration with new text.
Bootloader Monitor Commands	Updated the Table 3-1 table
Bootloader Monitor Response Codes	Added new description of the codes.
PC Utilities for Working with the Bootloader	• Updated Software Requirements to reflect latest Python requirements • Updated Boot.py Utility with new images and code syntax • Updated the Troubleshooting Guide to reflect the addition of Verify Python Version and Check Bootloader Execution with Terminal

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Trademarks

ISBN: 978-1-5224-4125-0

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820