TB003

An Introduction to KEELOQ® Code Hopping

Author: Kobus Marneweck
Microchip Technology Inc.

INTRODUCTION

Remote Control Systems

Remote control via RF or IR is popular for many applications, including vehicle alarms and automatic garage doors. Conventional remote control systems are based on unidirectional transmission and have limited security. More sophisticated devices based on bi-directional transmission are also available but, because of their high cost and certain practical disadvantages, they are not widely used in commercial remote control devices.

The popular unidirectional transmission systems currently have two very important security shortcomings: the codes they transmit are usually fixed and the number of possible code combinations is relatively small. Either of these shortcomings can lead to unauthorized access.

Code Scanning

The limited number of possible combinations available in most remote control systems makes it possible to transmit all possible combinations in a relatively short time. A hand held microprocessor-based system for this purpose (called a code scanner) can easily be constructed.

In systems using eight DIP switches (256 combinations), this scanning process can typically be accomplished in less than 32 seconds (when trying eight combinations per second). Even in systems using 16-bit keys (yielding roughly 65,000 combinations), only 2.25 hours would be required to try all possible combinations. It should also be noted that the scanner may gain access in far less than this maximum time—the average time would in fact be half of the total time.

Scanning is counteracted by increasing the number of possible code combinations. A 66-bit code will yield 7.3×10^{19} combination and will take 2.3×10^{11} years to scan.

Code Grabbing

A far easier way of gaining unauthorized access to a security system is freely available—such a unit is being advertised as a tool for the “legal repossession of vehicles.” To understand its operation, it is useful to know something about remote controls.

A remote control transmitter of the type normally used in vehicle security systems, is nothing but a small radio transmitter that transmits a code number on a certain frequency. This code number is normally generated by an integrated circuit encoder. The transmit frequency is normally fixed by legislation within a particular country, enabling anybody to build a simple receiver that can receive signals from all such transmitters.

It is a simple matter to build a circuit to record such transmissions captured by the receiver. Such a device is known as a code or key grabber. A would-be vehicle thief would typically lurk in a parking lot, waiting until a vehicle owner arms his alarm with a remote control. The key grabber would capture the transmitted code, enabling the thief to retransmit this code as soon as the owner leaves the parking lot. Typically, this would leave the alarm and/or immobilizer disabled and even the central locking unlocked.

The Solution

It is apparent that secure remote control systems can only be implemented if two conditions are met. The KEELOQ® code hopping system meets both these conditions with ease.

- A large number of possible combinations must be available.

  A 66-bit transmission code is used to make scanning impossible. The 32-bit encrypted portion provides for more than 4 billion code combinations. A complete scan would take 17 years! If the 34-bit fixed portion is taken into account, the time required for a complete scan jumps to 5,600 billion years!
- The system may never respond twice to the same transmitted code.

  The random code algorithm will never respond to the same code twice over several lifetimes of a typical system.

Every time a remote control button is pushed, the system will transmit a different code. These codes appear random to an outsider – there is no apparent relationship between any code and the previous or next code.

Once the system has responded to a valid code, about 65,000 valid codes will have to be received before the same code will be used again. If the remote control is used eight times daily, 22 years will pass before the system responds to the same code again - once! Therefore, a retransmitted code (like when a code grabber is used) will never activate the system.

The KEELOQ algorithm also features sophisticated synchronization techniques. The system will continue to function even if the transmitter is activated repeatedly while not in range of the receiver (as would happen if a child played with the remote control). If a button is pressed out of range more than 16 times, synchronization will be lost. However, two successive transmissions in range will restore synchronization. When no response occurs to a transmitter operation, the user's natural reaction is to press the button a second time. Synchronization will be restored when he does. Operation is totally transparent — the user may not even become aware that synchronization has been lost and restored.

These obvious security benefits are attainable at a cost comparable to existing fixed code systems. The revolutionary nature of the KEELOQ algorithm, full custom IC implementation, and reduced external component requirements help to make this level of cost effectiveness possible.

The KEELOQ Algorithm

KEELOQ is a proprietary block cipher based on a block length of 32 bits and a key length of 64 bits. The algorithm is characterized by a very economical hardware implementation, while retaining a level of security comparable to Data Encryption Standards (DES). This level of security makes it eminently suitable for code communication applications such as code hopping antitheft or access control devices.

Information regarding transmitter identity and synchronization is encoded so as to render it unintelligible to an outsider. For decoding, it is necessary to have the same 64-bit key originally used for encoding. Therefore, even though the decoder (which has the key) can identify the transmitter unambiguously, an outsider (who does not have access to the key and/or the algorithm) can glean no information at all from the transmissions.

As it is impossible to insert information into the system from outside, strategies used to attack FEAL and other DES-like ciphers are not usable against this system.

The KEELOQ algorithm is designed to make it impossible for a potential assailant to predict the next code that will be transmitted by a valid transmitter. Even if the assailant makes a reasonable guess regarding the way in which transmitted information changes with each transmission, the algorithm obscures this information sufficiently that the next code can not be anticipated. In particular, even if the transmitted information (before encoding) differs only in one bit from the information in the previous transmission, the next transmission will be totally different.

Checks exist that can be used to verify the security characteristics of an encoding algorithm and, in this instance, to determine whether the next transmitted code is predictable to any degree. The Avalanche Effect and a subset thereof, the Strict Avalanche Criterion, have been tested on the KEELOQ algorithm. The results give a good indication of the security offered by the system.

- Avalanche Effect (AE)

  A block cipher satisfies the AE if changing one bit of the information causes, on average, half of the bits in the transmission to change. In the KEELOQ algorithm, this implies that changing one bit in the function and/or synchronization information will cause an average of 16 of the 32 bits in the transmitted code to change.
- Strict Avalanche Criterion (SAC)

  The SAC requires that, if one bit of the encoded information is changed, each bit in the output must have a chance of 0.5 of changing as well. Consequently, the probability of guessing any one bit correctly is 0.5, and the probability of guessing an entire 32-bit string correctly is one in about 4,300,000,000!

  The tests involved using a random 64-bit key and a Gray counter (starting at zero) as input to the algorithm. In each case, the output was compared with a reference (SAC) or with the previous code (AE). In both cases, the results were as expected: For the AE, the average number of bits changed was 16.0 (50%), with a standard deviation of 2.83 (8.8%). For the SAC, each individual bit changed an average of 50% of the time, with a standard deviation of 8.8%.

DEFINITIONS USED IN CODE HOPPING

Transmitter Serial Number	Each transmitter is programmed with a unique 28- or 32-bit serial number at the time of transmitter manufacture. This ensures that each transmitter will be unique within a system.
Secret Key	This 64-bit secret key is generated by a key generation function from the 28- or 32-bit serial number or the 32- or 48-bit seed and 64-bit manufacturer's key as inputs. A manufacturer's key can be used to control the key generation function. The secret key is not readable and is never transmitted.
Seed	The seed is a 32- or 48-bit value that is programmed into the encoder. This can be programmed to be the same as one half of the key or be used in key generation. It is only transmitted when a specific button combination is activated and can be disabled once learning is completed.
Key Generation	The key generation function is used to generate a unique key for each transmitter from the serial number or seed value. It is preferable that the function is nonlinear. This function is performed by the programming station to generate keys to be programmed into transmitters.
Manufacturer's Key	The manufacturer's key is necessary in the receiver if a key generation function with a manufacturer's was used to generate the secret keys. The manufacturer's key must be programmed into the receiver during manufacture.
Normal Learn (Serial Number Derived)	The receiver uses the same information that is transmitted during normal operation to derive the transmitter's secret key, decrypt the discrimination value and the synchronization counter. All the transmitter information is then stored.
Secure learn (Seed Derived)	The transmitter is activated through a special button combination to transmit a stored 32- or 48-bit value (seed) that can be used for key generation or be part of the key. Transmission of the random seed can be disabled after learning is completed.
Discrimination value	The discrimination value is a 12-bit fixed portion of the encrypted word. It is used as a post decryption check.
Synchronization counter	A16-bit counter that is incremented on every activation of the encoder. It is stored on the receiver controller and compared to determine if a transmission is a previously received transmission, in which case it is ignored or falls within a forward window in which case it is accepted.

FEATURES

A full perspective of the capabilities of the KEELOQ system would involve describing the unique features of each device separately. However, the entire product range has certain characteristics that may or may not be applicable to a specific member of the product range. The most important characteristics are listed to enable the prospective user to get a global view of the KEELOQ system. The specifications for a particular encoder or decoder should be consulted to determine the applicability of these features to that device.

Encoders

Security

- Programmable 28/32-bit serial number
- Programmable 64-bit encryption key
- Each transmission is unique
- 66/67 bit transmission length
- 32-bit hopping code
- 34/35-bit fixed code (28/32-bit serial number, 4/0-bit function, VLOW, Rpt/2-bit CRC)
- Encryption key is read protected

Operating

- One (3.0V) or two (6.0V) Lithium battery operation
- One (9.0V or 12.0V) Alkaline battery operation
- 3 or 4 button inputs - 7 or 15 functions
- Selectable baud rate
- Automatic power down after transmission
- Battery low signal transmitted
- Nonvolatile synchronization data
- IR modulation capability

Other

- On-chip EEPROM
- On-chip oscillator and timing components
- On-chip reset circuit
- Button inputs have internal pull-down resistors
- Current limiting on LED output

Decoders

Security

- KEELOQ code hopping technology
- Secure storage of manufacturers key
- Secure storage of transmitters keys
- Normal learning mode and Secure learning mode
- Four or more transmitters can be learned

Operating

- 2.0V to 6.0V operation
- 4 MHz RC oscillator
- Learning indication
- Auto baud rate detection

Decoder

- Single chip decoder available
- On-chip EEPROM
- Four binary function outputs - 15 functions
- One or two wire serial interface
- Battery low indication

TYPICAL APPLICATIONS

- Automotive remote entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage openers
- Electronic door locks
- Identity tokens
- Burglar alarm systems
- Remote control toys/fixed code applications

ENCODER FUNCTIONS

General Description

The KEELOQ code hopping remote control encoders are intended for secure remote control systems. They are suitable for use in remote control applications using infrared (IR), microwave or other radio frequency (RF) transmitters.

The encoders have several basic modes of operation. Some of these modes may be combined in a particular device, and the means of selecting the mode may differ, but the principle of operation remains the same.

Unidirectional Authentication

Unidirectional authentication is used where it is impractical or cost prohibitive to use a bi-directional link such as remote keyless entry. In this mode, an encoder functions as a code generator for a transmitter. A suitable transmission medium (RF, ultrasonic, microwave, infrared, or magnetic coupling) must be provided in addition to the KEELOQ encoder to implement a complete link. The encoder is activated by a push button or by a magnetic field in the case of a transponder.

Bi-directional Authentication

Bi-directional authentication is used where a bi-directional link such as a direct connection is available. Bi-directional authentication mode implements an IFF (Identification Friend or Foe) system. In this mode, a 16/32-bit string (the challenge) is sent to the KEELOQ device. In the device, an encryption operation is performed on the challenge, using a 64-bit key. The resultant 16/32-bit string (the response) is then transmitted. This 32-bit string is unique for a given challenge and key. KEELOQ devices may contain several keys.

Transmission Format

The KEELOQ devices use a 66/67-bit transmission format. A 66-bit transmission is composed of a 32-bit encrypted string, a 28-bit fixed string, 4-bit function code, battery low indicator, and a repeat indicator. A 67-bit transmission is available on high-end encoders and is composed of a 32-bit encrypted string, a 28- or 32-bit fixed string, 4- or 0-bit function code, battery low indicator, and a 2-bit CRC. The fixed string is the serial number of the encoder and remains constant for all transmissions from a particular transmitter. However, the 32-bit encrypted string is unique for each transmission.

Transmitter Activation

The encoder has an internal power switch which turns on when any of the button inputs are taken high. When a button is pressed, the encoder is turned on and the inputs are sampled after a debounce delay. The encoder then transmits a code, based on the correct key, synchronization information, and function codes.

If the time-out option is selection, the encoder will shut-down after a complete transmission. This mode prevents battery depletion when a push button is inadvertently activated for an extended period. To activate the device again, the buttons have to be released and activated again.

With 28-bit serial number selected:

Hop code			Serial number			Function	Status/CRC
LSB	32 bits	MSB	LSB	28 bits	MSB	4 bits	2/3 bits

With 32-bt serial number selected:

Hop code			Serial number			Status/CRC
LSB	32 bits	MSB	LSB	32 bits	MSB	2/3 bits

Three data rates are used: 833, 1667, and 3333 bits per second. At the lower transmission rate, a complete transmission requires approximately 100ms, at the higher rate 50ms, and at the highest rate 25ms. All encoders will transmit the codes repeatedly while the transmitter is activated.

Special Features

Code Word Completion

Code word completion is an automatic feature that makes sure that the entire code word is transmitted, even if the button is released before the transmission is complete. A KEELOQ encoder powers itself up when a button is pushed and powers itself down after the command is finished, if the user has already released the button. If the button is held down beyond the time for one transmission, then multiple transmissions will result. If another button is activated during a transmission, the active transmission will be aborted and the new code will be generated using the new button information.

Blank Alternate Code Word

Federal Communications Commission (FCC) part 15 rules specify the limits on fundamental power and harmonics that can be transmitted. Power is calculated on the worst case average power transmitted in a 100ms window. It is therefore advantageous to minimize the duty cycle of the transmitted word. This can be achieved by minimizing the duty cycle of the individual bits and by blanking out consecutive words. Blank Alternate Code Word (BACW) is used for reducing the average power of a transmission. This is a selectable feature that is determined in conjunction with the baud rate selection bits. Using the BACW allows the user to transmit a higher amplitude transmission if the transmission length is shorter. The FCC puts constraints on the average power that can be transmitted by a device, and BACW effectively prevents continuous transmission by only allowing the transmission of every second or every fourth code word. This reduces the average power transmitted and hence, assists in FCC approval of a transmitter device.

Envelope Encryption Option

Envelope Encryption is a user selectable option which is meant to offer a higher level of security for a code hopping system. During a normal transmission with the envelope encryption turned off, the 28-bit serial number and 4-bit function code is transmitted in the clear (unencrypted). If envelope encryption is selected, then the serial number is also encrypted before transmission. The encryption for the serial number and 4-bit function code is done using a different algorithm than the transmission algorithm. The envelope encryption scheme is not nearly as complex as the KEELOQ algorithm and, hence, not as secure. When the envelope encryption is used, the serial number must be decrypted using the envelope key and envelope decryption. After the serial number is obtained, the normal decryption method can be used to decrypt the hopping code. All transmitters in a system must use the same envelope key.

Auto-shutoff

The Auto-shutoff function automatically stops the device from transmitting if a button inadvertently gets pressed for a long period of time. This will prevent the device from draining the battery if a button gets pressed while the transmitter is in a pocket or purse. This function can be enabled or disabled and is selected by setting or clearing the Auto-shutoff bit. Time-out period is approximately 25 seconds.

VLOW: Voltage LOW indicator

The VLOW bit is transmitted with every transmission and will be transmitted as a one if the operating voltage has dropped below the low voltage trip point. The trip point is selectable between two values, based on the battery voltage being used. This VLOW signal is transmitted so the receiver can give an indication to the user that the transmitter battery is low.

DECODER FUNCTIONS

General Description

The KEELOQ decoders can be used for secure remote control systems. To gain a full understanding of the modes of KEELOQ decoder operation, several concepts have to be understood.

Decoder Features

Output Activation

The function information contains information on the buttons that were activated. The function code is embedded in the encrypted portion of the transmission and is also transmitted in the clear if selected. The decoder will activate the switch outputs corresponding to the switch inputs on the encoder as long as the transmitter is activated. A minimum activation time of 500ms is used to allow for dropout in the signal. Buttons are usually assigned to different functions. In a vehicle alarm system one button might be used for arming and locking, another for disarming and unlocking and a third for trunk release. If any button is activated for more than say 2 seconds a panic siren can be activated.

Key Management

For a decoder to respond to an encoder's transmissions, the decoder has to have access to several items of information:

- The *serial number* which is unique for each transmitter. KEELOQ encoders feature 28- or 32-bit serial numbers.
- The *synchronization history* of that transmitter. This information is used to determine whether the transmission is a valid one, or whether it has been transmitted by a code grabber. The form in which this history is maintained makes it possible to re-synchronize the decoder with the transmitter, even if the transmitter has been pressed repeatedly out of range of the receiver.
- The *buttons* used to activate the transmitter.
- The *key* being used by that transmitter. All KEELOQ devices use 64-bit keys. This information is essential to enable the decoder to decrypt the transmission and gain access to the information contained in the encrypted code portion.
  - Single key system
    In a single key system the decoder stores a single key and uses that key for interpreting the transmissions from all transmitters. It follows that all transmitters to be used with that decoder, must be set up with the same key. A single key system is not very secure but the program is simplified and the storage requirements are less.
    The serial number is used to distinguish between different transmitters. The decoder still has to maintain separate synchronization information for each transmitter. This information is maintained in a separate location in the EEPROM memory for each transmitter. The history record for a particular transmitter is updated every time a valid transmission is received, enabling the decoder to keep track of each transmitter independently. Even if one transmitter is used regularly while another is stored away (with or without power), both transmitters will work the first time when activated.
  - Independent key system
    An independent key system is much more secure as the preferred method and is used in all KEELOQ decoders. In independent key systems, the decoder maintains a separate key for each transmitter. The serial number or derivative is used to locate the correct key. Once the correct location has been determined, the key is retrieved and used to decrypt the 32-bit encrypted portion. The correct history record is then retrieved and used to determine whether a valid code has been received.

Learning

Learning is a feature of KEELOQ decoders that allows the addition of new transmitters to the system without having to reprogram the system from outside.

The decoder's learning capability simplifies replacement of lost transmitters. When a transmitter is lost, the user can “teach” the decoder the key of a new transmitter. The previous transmitter's key will be written over, thereby excluding that transmitter from the system.

Once the self learning procedure has been followed, the receiver has learned the new transmitter's identity and (if applicable) the output functions that have to be activated for that transmitter. The new transmitter may then be used normally to activate the decoder.

Normal learning mode (Serial Number Derived)

- Transmission format in normal learn mode.

With 28-bit serial number selected:

Hop Code			Serial Number			Function	Status/CRC
LSB	32 bits	MSB	LSB	28 bits	MSB	4 bits	2/3 bits

With 32- bit serial number selected:

Hop Code			Serial Number			Status/CRC
LSB	32 bits	MSB	LSB	32 bits	MSB	2/3 bits

Operation

The user places the decoder in learning mode. When the first code word is received, the serial number is used to generate the transmitter's secret key that was programmed into the transmitter during the production stage. The secret key is used to decrypt the hopping code. The decoder then waits for a second transmission (must be activated a second time). The serial number is compared to the first received serial number. If equal the hopping code is decrypted and the validation checks performed. The final check is to check that the codes are sequential. All the transmitter information is then stored.

Secure learn mode (Seed Derived)

- Transmission format in secure learn mode

With 32 bit serial number selected:

Seed			Serial number			Function	Status/CRC
LSB	32 or 48 bits	MSB	LSB	28 or 12 bits	MSB	4 bits	2/3 bits

With 32 bit serial number selected:

Seed			Serial number			Status/CRC
LSB	32 or 48 bits	MSB	LSB	32 or 24 bits	MSB	2/3 bits

Operation

The user places the decoder in learning mode. During the first stage of learn, the user must press a specific button. The hopping code part of the transmission will be replaced by the 32/48-bit seed stored in the encoder. The key is derived from the seed instead of the serial number in this case. During the second stage of learning, any other button combination can be pressed. A normal hopping code transmission is sent during the second stage. The generated key is used to decrypt the hopping code, and all the transmitter information is stored.

Since the seed is only transmitted during the learning process, and is required to generate the key a normal transmission cannot be intercepted, a key generated and the hopping code decrypted to predict the next hopping code.

As a further security measure, the transmission of the random seed can be disabled after 1 to 128 operations of the transmitter once the transmitter has been learned. That means that even if someone had physical access to the encoder, it would not be possible to get the random seed which is needed for key generation. The disadvantage is that a transmitter cannot be relearned at a later stage.

Memory requirements

A code hopping system typically requires nonvolatile memory such as an EEPROM to store transmitter information. This allows information to be changed when a transmitter is learned and operated but ensures that the information will not be lost if power is removed. Since the receiver needs to store information on each transmitter, the number of transmitters is determined by the available memory size. A typical system requires 16 bytes to be stored for each transmitter.

Memory map:

Transmitter	
1	Learned
2	Learned
3	← Next learn position
~	
n	

A learning pointer can be used to point to the next available learning position. Once position n is reached, the pointer will wrap to position 1.

Transmitter replacement

The replacement of transmitters is a system implementation dependent. All transmitters can be erased by activating the learn input for 10 seconds. The wanted transmitters can then be relearned. Another method is to use a rotating buffer. Transmitters will be learned into sequential positions until the last position is reached. The next learn will then overwrite the first transmitter.

NOTES:

NOTES:

WORLDWIDE SALES AND SERVICE

AMERICAS

Corporate Office
Microchip Technology Inc.
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-786-7200 Fax: 480-786-7277
Technical Support: 480-786-7627
Web Address: http://www.microchip.com

Atlanta
Microchip Technology Inc.
500 Sugar Mill Road, Suite 200B
Atlanta, GA 30350
Tel: 770-640-0034 Fax: 770-640-0307

Boston
Microchip Technology Inc.
5 Mount Royal Avenue
Marlborough, MA 01752
Tel: 508-480-9990 Fax: 508-480-8575

Chicago
Microchip Technology Inc.
333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 630-285-0071 Fax: 630-285-0075

Dallas
Microchip Technology Inc.
4570 Westgrove Drive, Suite 160
Addison, TX 75248
Tel: 972-818-7423 Fax: 972-818-2924

Dayton
Microchip Technology Inc.
Two Prestige Place, Suite 150
Miamisburg, OH 45342
Tel: 937-291-1654 Fax: 937-291-9175

Detroit
Microchip Technology Inc.
Tri-Atria Office Building
32255 Northwestern Highway, Suite 190
Farmington Hills, MI 48334
Tel: 248-538-2250 Fax: 248-538-2260

Los Angeles
Microchip Technology Inc.
18201 Von Karman, Suite 1090
Irvine, CA 92612
Tel: 949-263-1888 Fax: 949-263-1338

New York
Microchip Technology Inc.
150 Motor Parkway, Suite 202
Hauppauge, NY 11788
Tel: 631-273-5305 Fax: 631-273-5335

San Jose
Microchip Technology Inc.
2107 North First Street, Suite 590
San Jose, CA 95131
Tel: 408-436-7950 Fax: 408-436-7955

AMERICAS (continued)

Toronto
Microchip Technology Inc.
5925 Airport Road, Suite 200
Mississauga, Ontario L4V 1W1, Canada
Tel: 905-405-6279 Fax: 905-405-6253

ASIA/PACIFIC

Hong Kong
Microchip Asia Pacific
Unit 2101, Tower 2
Metroplaza
223 Hing Fong Road
Kwai Fong, N.T., Hong Kong
Tel: 852-2-401-1200 Fax: 852-2-401-3431

Beijing
Microchip Technology, Beijing
Unit 915, 6 Chaoyangmen Bei Dajie
Dong Erhuan Road, Dongcheng District
New China Hong Kong Manhattan Building
Beijing 100027 PRC
Tel: 86-10-85282100 Fax: 86-10-85282104

India
Microchip Technology Inc.
India Liaison Office
No. 6, Legacy, Convent Road
Bangalore 560 025, India
Tel: 91-80-229-0061 Fax: 91-80-229-0062

Japan
Microchip Technology Intl. Inc.
Benex S-1 6F
3-18-20, Shinyokohama
Kohoku-Ku, Yokohama-shi
Kanagawa 222-0033 Japan
Tel: 81-45-471- 6166 Fax: 81-45-471-6122

Korea
Microchip Technology Korea
168-1, Youngbo Bldg. 3 Floor
Samsung-Dong, Kangnam-Ku
Seoul, Korea
Tel: 82-2-554-7200 Fax: 82-2-558-5934

Shanghai
Microchip Technology
RM 406 Shanghai Golden Bridge Bldg.
2077 Yan'an Road West, Hong Qiao District
Shanghai, PRC 200335
Tel: 86-21-6275-5700 Fax: 86 21-6275-5060

ASIA/PACIFIC (continued)

Singapore
Microchip Technology Singapore Pte Ltd.
200 Middle Road
#07-02 Prime Centre
Singapore 188980
Tel: 65-334-8870 Fax: 65-334-8850

Taiwan
Microchip Technology Taiwan
10F-1C 207
Tung Hua North Road
Taipei, Taiwan
Tel: 886-2-2717-7175 Fax: 886-2-2545-0139

EUROPE

United Kingdom
Arizona Microchip Technology Ltd.
505 Eskdale Road
Winnersh Triangle
Wokingham
Berkshire, England RG41 5TU
Tel: 44 118 921 5858 Fax: 44-118 921-5835

Denmark
Microchip Technology Denmark ApS
Regus Business Centre
Lautrup hoj 1-3
Ballerup DK-2750 Denmark
Tel: 45 4420 9895 Fax: 45 4420 9910

France
Arizona Microchip Technology SARL
Parc d'Activite du Moulin de Massy
43 Rue du Saule Trapu
Batiment A - ler Etage
91300 Massy, France
Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79

Germany
Arizona Microchip Technology GmbH
Gustav-Heinemann-Ring 125
D-81739 München, Germany
Tel: 49-89-627-144 0 Fax: 49-89-627-144-44

Italy
Arizona Microchip Technology SRL
Centro Direzionale Colleoni
Palazzo Taurus 1 V. Le Colleoni 1
20041 Agrate Brianza
Milan, Italy
Tel: 39-039-65791-1 Fax: 39-039-6899883

11/15/99

DNV Certification, Inc. USA — ANSI-RAB QMS ACCREDITED — DNV — DNV MSC The Netherlands Accredited by the RvA
ISO 9001 / QS-9000 REGISTERED FIRM

Microchip received QS-9000 quality system certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona in July 1999. The Company's quality system processes and procedures are QS-9000 compliant for its PICmicro® 8-bit MCUs, KEELOQ® code hopping devices, Serial EEPROMs and microperipheral products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001 certified.