AN1683

Introduction to Ultimate KEELOQ® Technology

Author: Cristian Toma
Microchip Technology Inc.

HIGH LEVEL DESCRIPTION OF KEELOQ® TECHNOLOGY

Microchip Technology has had a long history as a major supplier in the security industry primarily utilizing our proprietary, royalty-free KEELOQ technology, an industry proven technology used worldwide by leading manufacturers, to provide additional security to their applications for more than 15 years.

This application note gives a detailed description of Ultimate KEELOQ technology after reviewing the other KEELOQ technology offerings from Microchip. KEELOQ technology is a “code hopping” technology, which means that each transmission is unique (changes at every button press). At the core of this “code hopping” technology is a counter that increments with each button press. An encryption layer is then added to the packet. Such a system is known as an event-driven one, the event being the press of a button on the transmitter. A timer is used instead of a counter in the more advanced implementation of Ultimate KEELOQ technology. This timer runs at the same rate with a similar timer on the receiver side.

Table 1 below shows a comparison table with all available KEELOQ technology implementations.

TABLE 1: COMPARISON OF KEELOQ® TECHNOLOGY IMPLEMENTATIONS

KEELOQ® Technology Version	Security Level	Encryption Engine	Encryption Key Length	Transmission Length	Synchronization
Classic KEELOQ Technology	Medium	NLFSR	64	66	Counter
Advanced KEELOQ Technology	High	AES	128	168	Counter
Ultimate KEELOQ Technology	High	AES	128	192	Counter + Timer

1.0 REVIEW OF CLASSIC KEELOQ TECHNOLOGY

1.1 Synchronization counter

The synchronization counter is the heart of the hopping code algorithm. It increments every button press. The synchronization information is used at the decoder to determine whether the transmission is valid or whether it is a repetition of a previous transmission. Repetitious codes are rejected to safeguard the system against code grabbers.

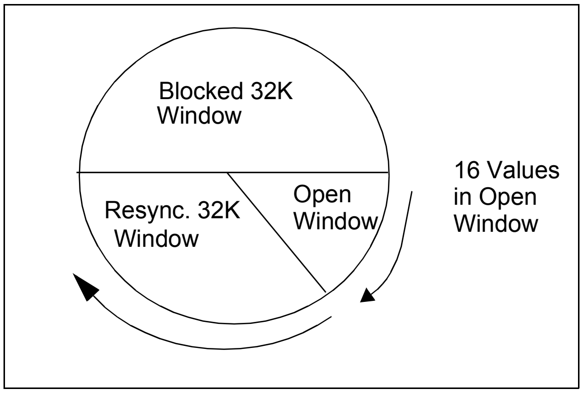
The transmitting encoder has a 16-bit synchronization counter and its value is stored in EEPROM. The synchronization counter value received is stored in the decoder's EEPROM every time a valid transmission is received from a particular encoder. When a transmission is received from the same transmitter it is possible to quickly verify whether the transmission is valid. A replayed code which was previously captured from the legitimate user's previous transmission will result in a synchronization counter value that is lower than or equal to the last known good value received.

Provision must be made for the transmitter being pressed while out of range of the decoder. The decoder does this by allowing two 'synchronization windows'. The single operation window is a reception of a transmission where the synchronization counter falls within a small window (a typical value of 16 units), higher than the previous counter value received. The reception of such a signal will result in an immediate counter update by the decoder and the appropriate outputs being activated.

If the transmitter's counter rolls outside the window implemented in the receiver firmware, resynchronization needs to take place. The Resynchronization Window is half of the total counter range (32K). When the decoder receives a transmission with a synchronization counter value more than the open window above the stored counter value and less than 32,768 counts above the stored value, the decoder temporarily stores the value of the synchronization counter received. If the next transmission received has a sequential synchronization counter value, the decoder resynchronizes on the last transmission received, storing the latest counter in EEPROM and activates the appropriate outputs.

If any of the above tests fail, the transmission received is discarded.

FIGURE 1: SINGLE OPERATION WINDOW



1.2 Typical Packet

A typical Classic KEELOQ technology packet consists of two parts. One part is being sent in plain text and the other is sent encrypted. Sending part of the message in plain text allows for backwards compatibility with fixed code receivers. Some of the information that is being sent in plain text is contained inside the encrypted section and can be used as a post-decryption check.

1.2.1 SERIAL NUMBER

This is a unique number that is specific to each individual encoder. Its main purpose is to differentiate between encoders. The encoder serial number is transmitted every time a button is pressed. The serial number is transmitted unencrypted as part of the transmission.

1.2.2 FUNCTION CODE

The function code contains a bit field indicating the buttons pressed on the encoder.

1.2.3 ENCRYPTED SECTION

This is the actual "hopping code" portion (32-bit wide for KEELOQ Classic technology). This contains a copy of the function code, the discrimination value and the synchronization counter. This copy of the function code is checked against the copy sent in plain text as a step in the post-decryption checking. The discrimination value is also checked. In a typical implementation, the discrimination value is the 10-bit LSb of the serial number. The synchronization counter is checked against the value that the decoder is storing for each learned encoder.

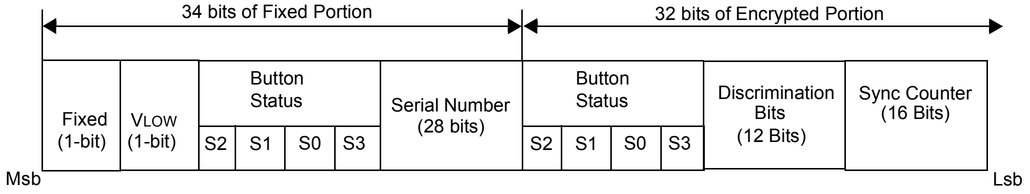
The encrypted portion contains:

- 16-bit synchronization counter. This is at the base of Classic KEELOQ technology rolling code
- 12 discrimination bits. These are typically the 12 LSb of the serial number. This value is used as post-decryption check
- 4-bit information about the button (or button combination) that caused the transmission. Please note that this information is also sent in the fixed portion. Like the discrimination value, this information can be used for post-decryption check

1.2.4 FIXED SECTION

- 32-bit serial number, specific to each individual encoder. Its main purpose is to differentiate between encoders
- 4-bit information button information
- 1-bit low-voltage indication. This bit indicates that the battery voltage has dropped below a set level

FIGURE 2: CLASSIC KEELOQ® TECHNOLOGY PACKET STRUCTURE



1.2.5 SEED PACKET

The seed packet is a special transmission sent when a special key combinations is pressed. Instead of the encrypted portion, the seed value is transmitted. The seed can be 32, 48, and 60-bit wide. Depending on the actual implementation, the structure of the seed packet can vary.

1.3 Key Management and Key Generation Schemes

1.3.1 SIMPLE LEARN

The Simple key generation scheme is the simplest scheme that a KEELOQ technology system supports. When using simple key generation, one single key is used by all encoders and the transmitters are differentiated only by the serial number.

It is very important that the user understands exactly what the implications of using such a key generation scheme are. This could be a potential security risk. If any encoder is compromised and the encryption key is found, then all the encoders are compromised, because they use exactly the same key.

EQUATION 1: SIMPLE KEY CALCULATION SCHEME

$$K_{Encryption} = K_{Manufacturers\ Code}$$

$$Where$$

$$K_{Encryption} : the\ encryption\ key(for\ each\ encoder)$$

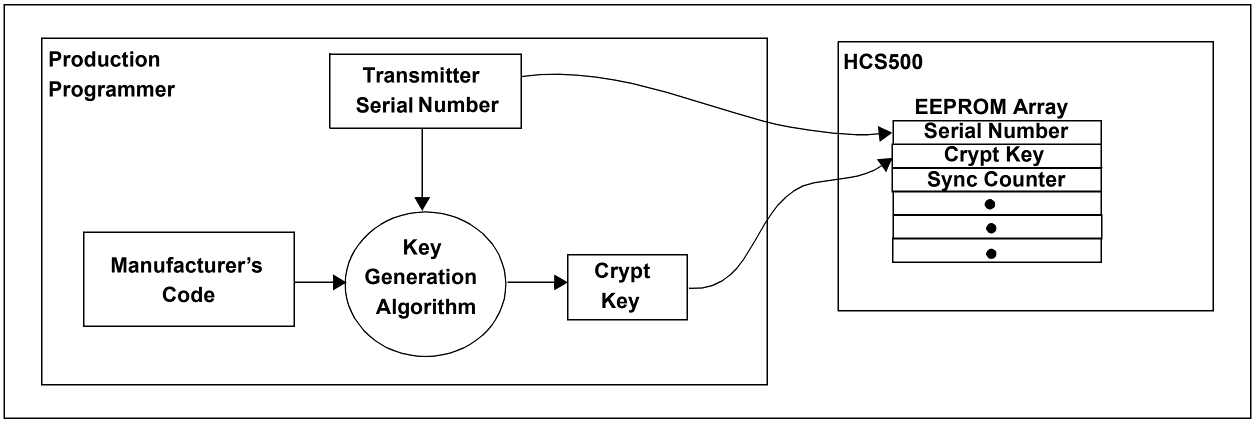
$$K_{Manufacturers\ Code} : the\ manufacturer\ code$$

1.3.2 NORMAL LEARN

When using the normal learning mechanism, the decoder uses the manufacturer code and the serial number to calculate the decryption key for each transmitter.

The Normal key generation scheme is the common key generation scheme for KEELOQ technology systems. During Normal Learn, a master key is used (known as the “manufacturer code”).

FIGURE 3: CREATION AND STORAGE OF CRYPT KEY DURING PRODUCTION



Using the serial number of each encoder and the manufacturer code, the unique encryption key for each encoder is calculated. The encoder stores only the serial number and the calculated encryption key. The decoder needs to be programmed with this manufacturer code in order to be able to calculate individual encryption keys. To calculate the encryption key, the 28-bit serial number is padded with `0x6000000` and `0x20000000` and decrypted using the manufacturer code as the decryption key. This operation is done twice, in order to calculate the high part and the low part (MSB and LSB) of the encryption key.

EQUATION 2: UPPER 32 BITS OF THE ENCRYPTION KEY

$$K_{Device} = \boldsymbol{D}(Manuf.Code, Serial\ number\ |0x6000000)$$
$$for\ the\ upper\ 32\ bits$$

EQUATION 3: LOWER 32 BITS OF THE ENCRYPTION KEY

$$K_{Device} = \boldsymbol{D}(Manuf.Code, Serial\ number\ |0x20000000)$$
$$for\ the\ lower\ 32\ bits$$

1.3.3 SECURE LEARN

The Secure key generation scheme is a more advanced key generation scheme. When using the normal key generation scheme, the key is generated from the serial number and the manufacturer code. Since the serial number is transmitted in any packet, one part of the key generation scheme is always exposed. But an even more secure method is to generate a random number (called "seed"). Depending on the length of the seed, there are three key generation schemes: 32-bit seed, 48-bit seed and 60-bit seed.

Figure 4 through Figure 6 show how the secure key generation technique described is implemented and how the different seed lengths of the various encoders are handled.

FIGURE 4: SECURE KEY CALCULATION FOR 32-BIT SEED

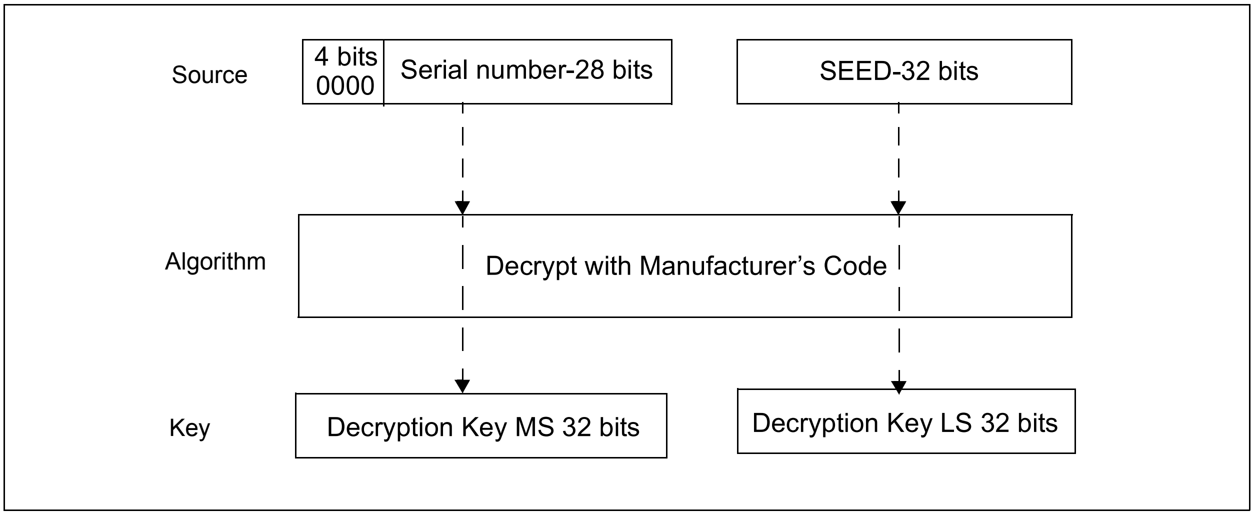

Source
4 bits
0000
Serial number-28 bits
SEED-32 bits
Algorithm
Decrypt with Manufacturer's Code
Key
Decryption Key MS 32 bits
Decryption Key LS 32 bits

FIGURE 5: SECURE KEY CALCULATION FOR 48-BIT SEED

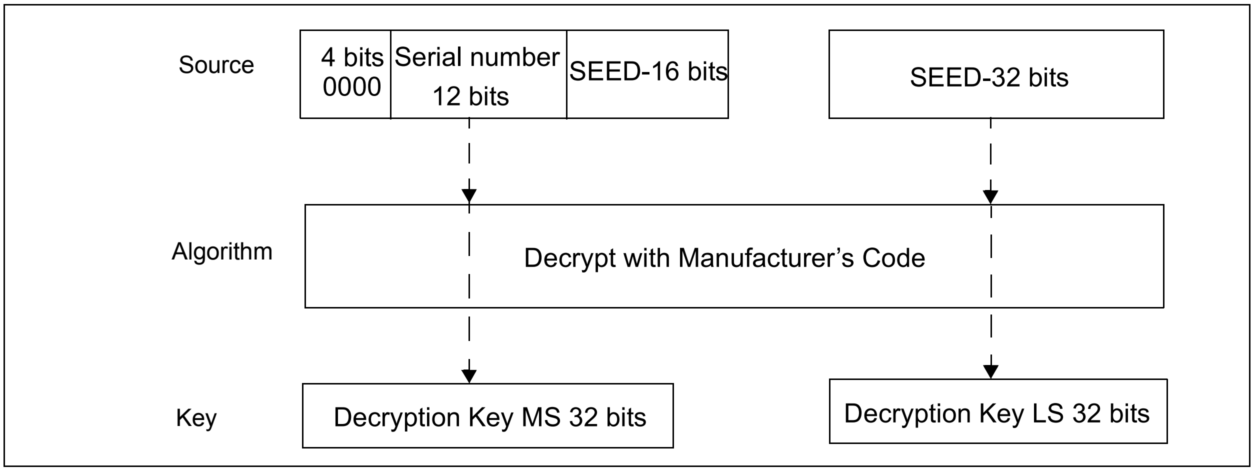
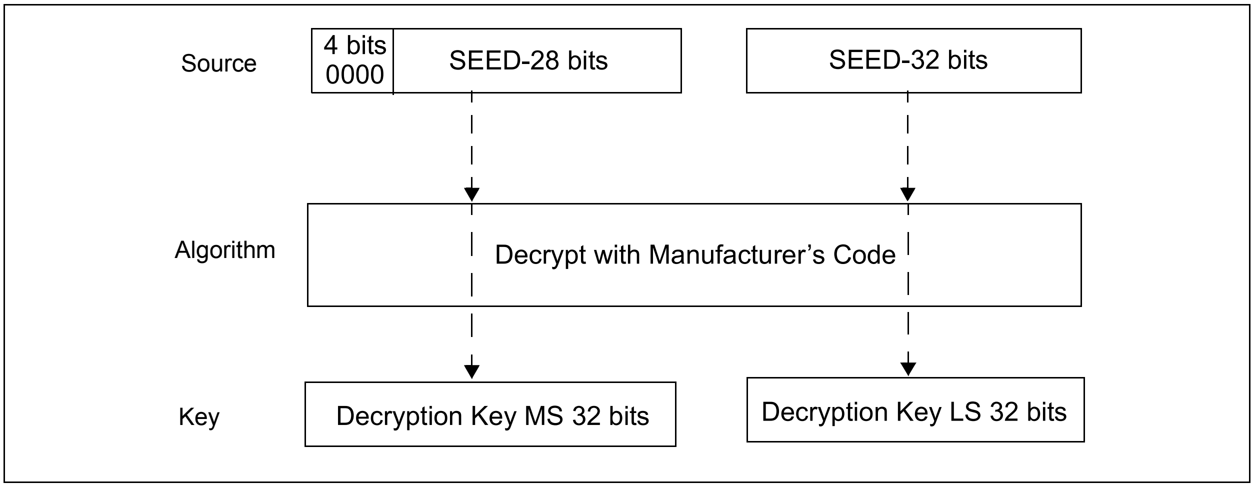

Source
4 bits
0000
Serial number
12 bits
SEED-16 bits
SEED-32 bits
Algorithm
Decrypt with Manufacturer's Code
Key
Decryption Key MS 32 bits
Decryption Key LS 32 bits

FIGURE 6: SECURE KEY CALCULATION FOR 60-BIT SEED


Source
4 bits
0000
SEED-28 bits
SEED-32 bits
Algorithm
Decrypt with Manufacturer's Code
Key
Decryption Key MS 32 bits
Decryption Key LS 32 bits

During normal operation, the seed is not transmitted. The only time when the seed is transmitted is during the learning/pairing phase. Thus, the information that is used to generate the encryption key is kept confidential. Some implementations take the security level even further, by allowing the seed to be transmitted only for a limited period (in which the system is installed) and then disabling this feature.

1.4 Transmission Modulation Format

Typical modulation formats used by KEELOQ encoders are:

- Pulse-Width Modulation (PWM)
- Manchester (MAN)
- Variable Pulse-Width Modulation (VPWM)
- Pulse Position Modulation (PPM)

2.0 REVIEW OF ADVANCED KEELOQ TECHNOLOGY

Advanced KEELOQ technology is similar to Classic KEELOQ technology, except for the fact that it provides a higher level of security due to the stronger encryption algorithm. The encryption itself is handled by the AES encryption algorithm (versus the NLFSR used in the Classic KEELOQ technology). The encrypted portion is 128-bit (versus the 32-bit encrypted portion used by the Classic KEELOQ technology). The encryption key is 128-bit (versus the 64-bit encryption key used by Classic KEELOQ technology). Apart from this, there are a number of similarities between Advanced KEELOQ technology and Classic KEELOQ technology. Advanced KEELOQ technology is very similar to Classic KEELOQ technology; the main distinction being that Advanced KEELOQ technology replaces the KEELOQ technology algorithm with the industry standard AES-128 algorithm, which has been adopted by industry, as the preferred encryption standard.

2.1 Packet Format

Depending on the actual implementation of Advanced KEELOQ technology, there can be different packet formats. However, all share the same main features, like the counter and the AES encryption.

2.2 Key Management and Key Generation Schemes

2.2.1 SIMPLE LEARN

The Simple Key Generation Scheme is the same as the one used in Classic KEELOQ technology.

EQUATION 4: SIMPLE KEY CALCULATION SCHEME

$$Encryption\ Key = Manufacturer\ Code$$

2.2.2 NORMAL LEARN

Advanced KEELOQ technology maintains the same Normal (Serial Number Derived) Learn scheme as used in Classic KEELOQ technology. The key is however padded with a different vector since the encryption algorithm uses 128-bit blocks.

EQUATION 5: ADVANCED KEELOQ® TECHNOLOGY KEY CALCULATION SCHEME

$$(0xA5A5A5A5 - 5A5A5A5A - SerialNumber - 00000000)_{Decrypt(Key = \ Manufacturer\ Code)} = \ Encryption\ Key$$

3.0 ULTIMATE KEELOQ TECHNOLOGY THEORY

Ultimate KEELOQ technology is a new patented Microchip security and authentication solution that adds an on-board free running timer. When a button is pressed, a snapshot of its internal timer value is captured and sent inside the encrypted data packet. The receiver also has an on-board timer at its end. When a transmitter is learned to a receiver, the receiver stores relevant information, such as the timer value when synchronized, the last received time-stamp and the resynchronization counter.

In an Ultimate KEELOQ technology system, both the transmitter and the receiver are having on-board free-running timers. These are either crystal-driven (an external crystal connected to TIMER1 oscillator) or counting the WDT periods. Depending on the actual implementation, any time-keeping source can be used, provided that it has adequate tolerance and stability. The exact timer values at both ends will be different, since they started running at different times. However, both timers will run at the same speed. When a transmitter is learned by a receiver, the receiver gets a snapshot of its own timer value and of the transmitter's timer value. It then stores the delta value (the difference) between the two timer values. At this point, both timers are synchronized. When a transmission is received, the receiver takes the time-stamp inside the transmitted packet and adds the delta time stored for that particular transmitter. The result is then compared with the receiver timer. In an ideal situation, the two values will match perfectly. However, the timers at both ends have limited accuracy, so the "estimated" timer value and the actual timer on the receiver side will most often not have the exact same value, but rather close-by values.

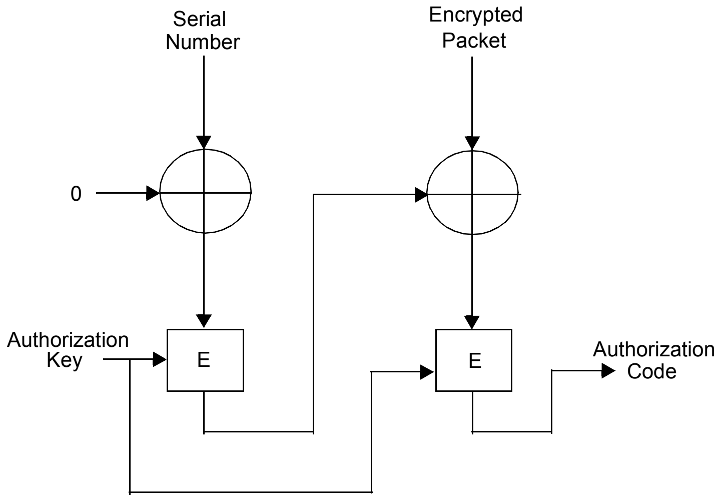
3.1 Separation of Security and Authentication

The Ultimate KEELOQ technology system separates the concept of security from the concept of authentication. The Ultimate KEELOQ technology packet contains the serial number, the encrypted section, and an authorization code).

At the end of each transmission packet, an authorization code is being sent. This is calculated using the cipher block chaining. At each step, one block of 128 bits of data is being encrypted (using AES) using the authentication key as the encryption key. The resulting crypto text is then XOR'ed with the next data block, and then the result is used as input for the next encryption step, using the same authentication key and so on until the end of the data is reached. Each block of data is XOR'ed with the previous one (padded with zeros if it's the first one). Thus, each cipher text block is dependent on the previous one.

For KEELOQ Ultimate technology we need to use two encryption steps to calculate the authorization code because the data consists of two 128-bit blocks. For the first block, we use the serial number padded with zeros. For the second block, we use the 128-bits that make up the encrypted portion of the transmitted packet.The 32-bit authorization value that is placed in the transmitted packet is the 32-bit lower significant bits of the resulting authorization code. The encryption key that is used for authorization code calculations is different from the encryption key used in the same packet and is called the authorization key.

FIGURE 7: AUTHORIZATION CODE CALCULATION ALGORITHM USED BY ULTIMATE KEELOQ® TECHNOLOGY



3.2 Advantages of Time-stamped Transmissions

The Ultimate KEELOQ technology provides the highest level of security in the KEELOQ technology line. It is also the most complex one.

Upon reception of an Ultimate KEELOQ technology packet, the receiver has to do a series of rather complex operations before validating a packet. But at the same time, its operation is completely transparent to the user.

Every Ultimate KEELOQ technology packet sent over the air contains a time-stamp. This time-stamp is validated by using a synchronized timer on the receiver side. The receiver checks this time-stamp against the synchronized timer. An acceptance window is then applied, the receiver allowing only a small window of time difference between the two timer values.

Another advantage of Ultimate KEELOQ technology is the possibility to use a transmitter with any number of receivers. This is due to the fact that the receiver is validating time-stamps of a known, authenticated transmitter. This was not possible with Classic and Advanced KEELOQ technology since their operation is based on the synchronization counter. Operating one (Classic or Ultimate) transmitter with a different receiver will result in loss of synchronization. An Ultimate KEELOQ technology transmitter can be safely operated with any number of receivers.

3.3 Timer Drift and the Acceptance Window

Immediately after synchronization, both timers are running synchronously. But over time, any slight tolerance in the oscillator frequency will produce an error that will accumulate over time. Most of the time, the timers at both ends (transmitter and receiver) will not be perfectly synchronized, but rather having a predictable deviation. When dealing with short periods of time, the error is insignificant and the receiver will only allow a very small window of timer error. However, at long periods of time (say weeks to a few months), the total amount error that has accumulated over time is significantly larger. Therefore, the receiver needs to allow for a very large error when comparing the values of the two timers (transmitter and receiver). Is up to the system designer to set these limits and perhaps set a maximum error limit that the receiver will accept.

FIGURE 8: GRAPHIC OF TIMER DRIFT OVER TIME

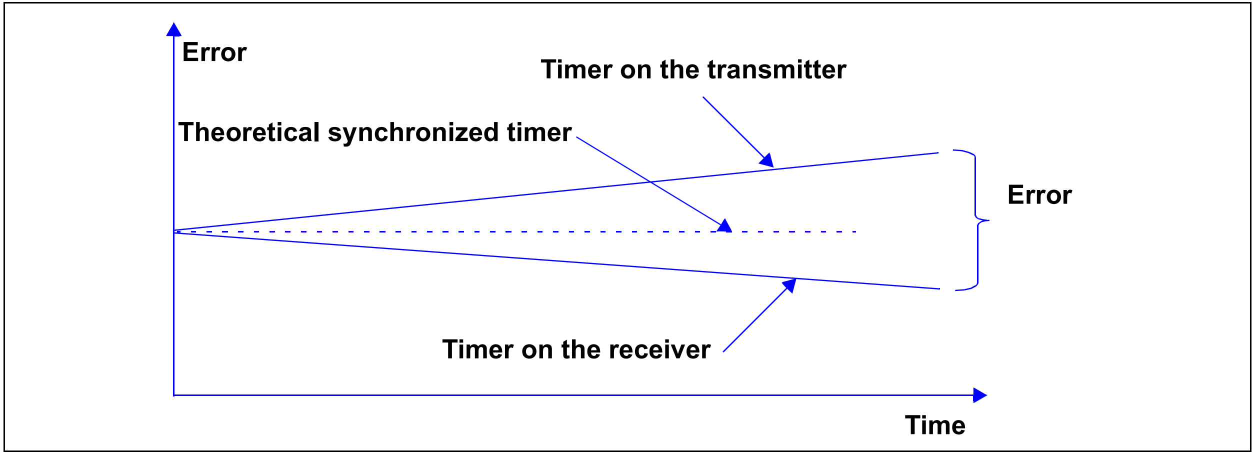
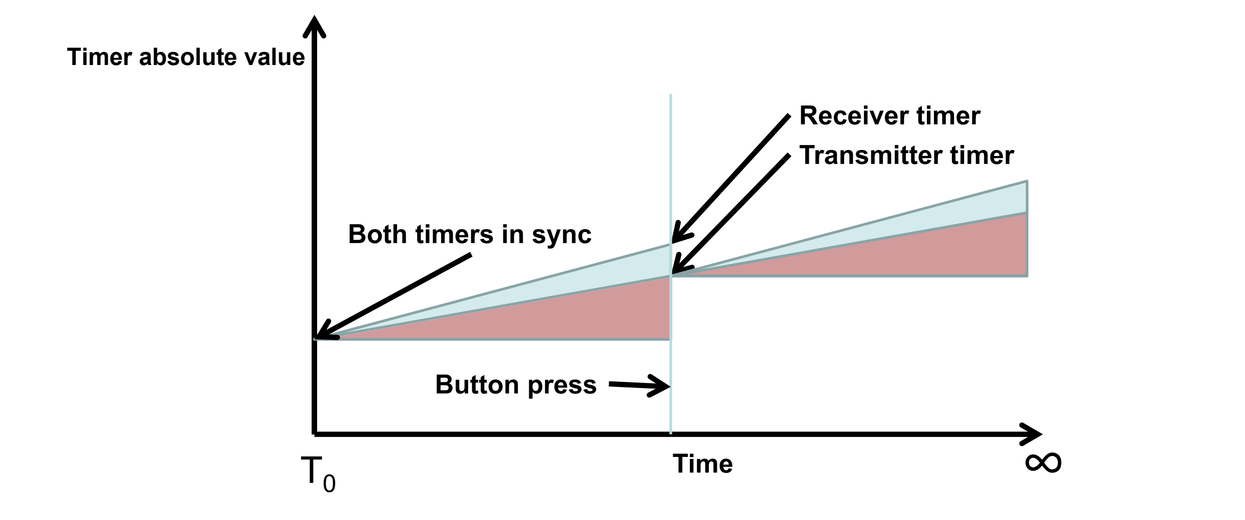


FIGURE 9: EXAMPLE OF TIMER DRIFT ADJUSTMENT AFTER A RESYNCHRONIZATION



3.3.1 TRANSMITTER RESYNCHRONIZATION

Timers will continue to run as long as they have constant and uninterrupted power supply. But there are times when the power needs to be interrupted for maintenance (such as changing the battery on the transmitter) or simply a power failure (such as a mains power interruption on the receiver side). Inevitably, when one of the timers loses power, its value will be lost. On the transmitter side, the timer will re-start from the last time-stamp value (saved upon a button press). Still, its value is not synchronized. The transmitter needs to have a way to signal the receiver that the transmitter lost its power supply and its timer is not synchronized. The receiver will then resynchronize that transmitter by adjusting the delta value. However, this must be signaled in a secure way so that only a legitimate transmitter will be able to send a resynchronize request. This is done by implementing a counter on the transmitter. The value of this counter is stored in the nonvolatile memory. Each time the transmitter chip powers-up, it reads this value, increments it and saves it back to the nonvolatile memory. The value of this counter is being transmitted inside the data packet. We call this counter “resynchronization counter”. The receiver also stores a copy of it in its nonvolatile memory. When the receiver sees that this resynchronization counter has advanced, it automatically re-adjusts the delta value between the receiver timer and the transmitter timer. Thus, the transmitter will be resynchronized. If the timers have drifted outside of the window the user will have to force the increment of this counter by performing a Reset of the transmitter, by removing the battery temporarily in order to gain access.

3.3.2 RECEIVER RESYNCHRONIZATION

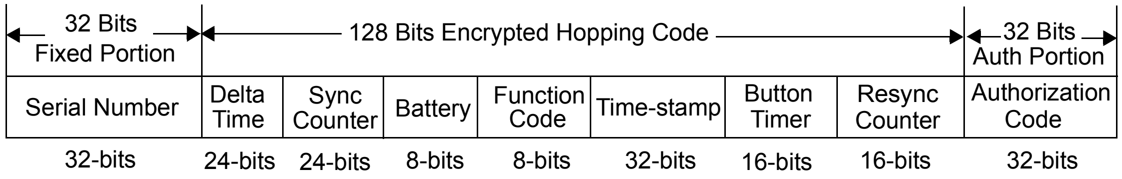
The receiver can also encounter a power loss. In this case, resynchronization is a little bit more complex. The receiver has only one timer. The synchronization with learned encoders is done by using a delta value between the receiver and the received time-stamp sent by each encoder. While the receiver does not have power, it has no way of knowing the exact amount of time that has passed. In order to have a proper resynchronization mechanism, the receiver needs to have an on-board real-time clock with a battery back-up. In the event of a power loss, the receiver still has the timer synchronized. After a power-up, the receiver will first read the time information from the real-time clock. It will then adjust the internal timer of the receiver. This way, the receiver will have the correct timer value and all the transmitters will continue to work correctly.

4.0 ULTIMATE KEELOQ TECHNOLOGY IMPLEMENTATION

A normal transmission consists of 192 bits of data.

A typical Ultimate KEELOQ technology packet consists of three parts: the serial number (transmitted in plain text), the encrypted section, and the authorization code. The encrypted section contains a 32-bit time-stamp, an 8-bit function code and a 24-bit sync code (similar to the Classic KEELOQ technology synchronization counter). It also contains a 24-bit delta time (representing the time since the last button press), an 8-bit battery level indication, a button timer (representing the total time a button was pressed), and a resync counter used when the transmitter has lost its power.

FIGURE 10: ULTIMATE KEELOQ® TECHNOLOGY NORMAL PACKET STRUCTURE

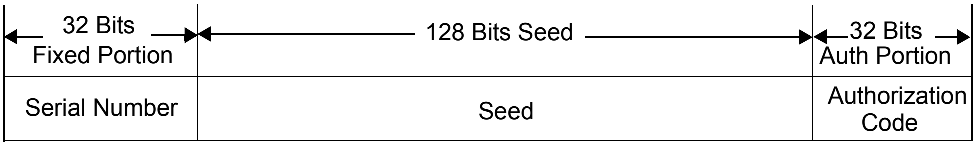


32 Bits Fixed Portion	128 Bits Encrypted Hopping Code							32 Bits Auth Portion
Serial Number	Delta Time	Sync Counter	Battery	Function Code	Time-stamp	Button Timer	Resync Counter	Authorization Code
32-bits	24-bits	24-bits	8-bits	8-bits	32-bits	16-bits	16-bits	32-bits

The seed packet is similar to the typical packet, except that instead of the encrypted section it will transmit the seed value. This packet is only transmitted during the secure learn phase (if using secure learn) and it is typically activated by a special button combination (user-defined).

When sending the seed packet, the serial number will be sent as 0xFFFFFFFF.

FIGURE 11: ULTIMATE KEELOQ® TECHNOLOGY SEED PACKET STRUCTURE



32 Bits Fixed Portion	128 Bits Seed	32 Bits Auth Portion
Serial Number	Seed	Authorization Code

Note: In the Seed code word, the serial number is sent as 0xFFFFFFFF.

Serial number

The serial number is 32-bit wide and is being sent in plain text.

Delta Time

This is the time since the last button was pressed. This information is useful when implementing features like pressing a button twice to activate a certain feature (like a double-click). Also, it could be used to double check on the receiver side if the last button press coincides with the information that the receiver has stored.

Sync

This is a synchronization counter. It works in a similar way as the counter used in classic KEELOQ technology systems. The system designer can choose whether to use it or not, for an extra security feature. An Ultimate KEELOQ technology transmitter can work with more than one receiver, if the user does not use the sync counter.

Battery Level

This is a field that indicates the actual battery voltage on the transmitter battery. A typical implementation would use the ADC peripheral. But this might vary according to implementation and on-board available peripherals.

Function Code

This field indicates which button was pressed. Since this is an 8-bit field, up to 256 individual buttons combinations can be implemented (on a software implementation, Ultimate KEELOQ technology MCS devices are limited to hardware capability).

Timer

This is the actual timer used for the Ultimate KEELOQ technology time synchronization mechanism. The timer value typically increments once every 250 ms, but any increment can be used as long as the receiver and transmitter increments the timer at the same frequency.

Button Timer

This is a timer that increments while you keep a button pressed. This is a 16-bit value that increments with each transmitted packet.

Resync Counter

This is a counter that increments each time the transmitter powers-up. This counter is used for automatic resynchronization when the transmitter loses power. Typical cases would be a low-battery condition or a change of the battery.

The data is sent in this order:

- Authorization code (32-bits wide)
- Encrypted portion (128-bits wide)
- Serial number (32-bits wide)

All data is transmitted LSB first.

4.1 Transmitter Time Source Examples

4.1.1 TMR1 PERIPHERAL WITH A 32.768 kHz OSCILLATOR

An Ultimate KEELOQ technology system involves the use of two timers, both on the transmitter side and receiver side. A typical implementation uses a timer derived from a 32.768 kHz external crystal. The external crystal is connected to the TIMER1 dedicated oscillator circuit. Timer1 is a 16-bit timer and under normal conditions (no prescaler) will have an overflow period of two seconds (32768 counts per second, overflow at 65536 counts).

In order to save power, the processor needs to spend most of its time in Sleep mode. So instead of waking up every two seconds, performing the timer operations and going back to Sleep, a prescale ratio can be used. For example, a Prescaler of 1:8 will result in a timer overflow period of 16 seconds. The processor will only wake-up from Sleep once every 16 seconds, increment a counter and go back to Sleep. Further precision can be obtained at any moment by taking information from the TIMER1 register.

4.1.2 WDT PERIPHERAL

Another clock source that Ultimate KEELOQ technology can use is the Watchdog Timer (WDT). This is a timer that ensures that the processor is working properly. This WDT has an independent RC internal oscillator.

The PIC16F1XXX enhanced core has an on-board hardware Watchdog Timer with configurable time-out period from 1 ms to 256 seconds. Depending on the actual device, the WDT operation can vary. The WDT timer can operate during Sleep and can wake-up the device from Sleep mode. The timer required by Ultimate KEELOQ technology can be implemented by periodically putting the transmitter in Sleep mode while having the Watchdog Timer active. When the WDT times-out, it will wake the processor from Sleep, the processor will the increase the timer, perform other required tasks and then go back to Sleep. The operation will repeat indefinitely with the processor waking-up after each Watchdog time-out period, increasing the timer value and immediately going back to Sleep.

4.1.3 USING A 32.768 kHz CRYSTAL

The crystal oscillator has a limited precision and stability. Likewise, the WDT period is derived from an internal precision-limited oscillator. The actual oscillating frequency will vary from device to device and depending on temperature. On the receiver side, the timer will have the same behavior. It is important that the designer understands how the precision and the stability are impacting the oscillating frequency.

While a crystal oscillator will be labeled as 32.768 kHz, its real oscillating frequency will never be this exact value, but rather a close value to the one specified. This is due to its crystal structure and manufacturing process.

There are several factors that influence the actual oscillating frequency of a crystal oscillator.

- The initial frequency error, expressed in parts-per-million:

EQUATION 6: DEFINITION OF PPM (PARTS-PER-MILLION) ERROR

$$\varepsilon = \frac{F_r - F_s}{F_s} \bullet 10^6$$

$Where:$

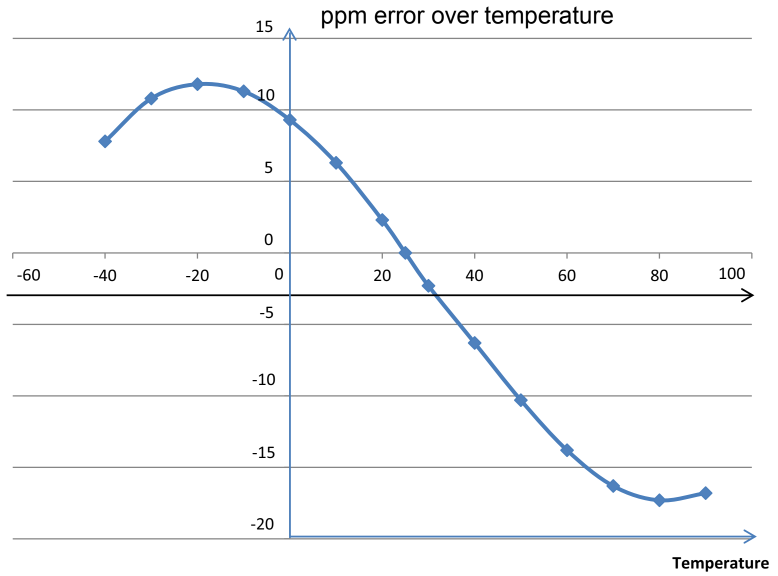
$F_r = \text{real } frequency$

$F_s = specified\ frequency$

This is from the manufacturing process and its value will be characteristic for a specific unit. It is also known as “frequency tolerance”. Common frequency tolerances of a crystal range from +/- 5 ppm to +/- 100 ppm. In general, a tighter tolerance will impact the cost of a crystal, raising its price. The most common tolerance used is 20 ppm.

The temperature drift will impact the real oscillating frequency. The crystal specifications are given at 25°C. But in normal operating temperatures, other than 25°C, the temperature drift can add 10-15 ppm. The following figure shows a typical frequency deviation. The initial tolerance of a crystal is given at 25°C. Depending on the actual operating temperature, the tolerance will increase/decrease by up to 15 ppm.

FIGURE 12: TYPICAL CRYSTAL FREQUENCY DRIFT OVER TEMPERATURE



Crystal aging will affect the oscillating frequency over a very long period of time (years). Aging is typically 2-5 ppm over the life of the crystal.

All the above parameters will vary from manufacturer to manufacturer and from unit to unit. For the exact specifications, one should consult the manufacturer’s product specifications.

This is a typical window calculation example. We start with a typical 30 ppm crystal oscillator. This is having a +30 ppm to -30ppm initial tolerance. So, in our calculation, we will assume a worst-case scenario where the transmitter is running 30 ppm faster and the receiver is running 30 ppm slower. The actual oscillating frequency on the transmitter will be:

EQUATION 7: FREQUENCY CALCULATION FOR A 32.768 kHz CRYSTAL RUNNING 30 PPM FASTER

$$f_{TX=}\ 32768\ Hz + \frac{30\ ppm * 32768\ Hz}{10^6} = 32768.98304\ Hz$$

Likewise, the frequency on the receiver will be:

EQUATION 8: FREQUENCY CALCULATION FOR A 32.768 kHz CRYSTAL RUNNING 30 PPM SLOWER

$$f_{RX=}\ 32768\ Hz - \frac{30ppm * 32768\ Hz}{10^6} = 32{,}767.01696\ Hz$$

This means that the transmitter is running 0.98304 Hz faster than required and the receiver will run 0.98304 Hz slower than required. Based on these figures, we can estimate the acceptance window for a given time period since the last resynchronization.

Acceptance Window

The number of units that have accumulated over a period of one day, due to this frequency error:

EQUATION 9: WORST-CASE TIMER ERROR CALCULATION FOR ONE DAY PERIOD

$$60s * 60\ min * 24\ hours * 30\ ppm = 2.592\ seconds$$

The number of timer units is dependent on the timer tick interval. For a typical implementation that uses 250 ms tick interval, the equivalent number of counts is:

EQUATION 10: WORST-CASE TIMER ERROR CALCULATION FOR ONE DAY PERIOD, MEASURED IN TIMER UNITS

$$\frac{2.592\ seconds(deviation)}{0.25\ seconds\ (tick)} \cong 10\ units$$

Similarly, we can calculate for one month interval:

EQUATION 11: WORST-CASE TIMER ERROR CALCULATION FOR ONE MONTH PERIOD

$$60s * 60\ min * 24\ hours * 31\ days * 30\ ppm = 80.352\ seconds$$

This results a number of timer units of:

EQUATION 12: WORST-CASE TIMER ERROR CALCULATION FOR ONE MONTH PERIOD, MEASURED IN TIMER UNITS

$$\frac{80.352\ seconds(deviation)}{0.25\ seconds\ (tick)} \cong 321\ units$$

Please note that the above figures are only for the transmitter side (considering a 30 ppm maximum tolerance). The same amount of error could exist on the receiver side (considering the same ppm error on the receiver side). Thus, the actual values of the error will be double the amount calculated above.

The above calculation was done considering a constant temperature at both ends (transmitter and receiver). However, in practice, both ends will run at different temperatures. A typical case would be the receiver located inside of a vehicle or garage door opener and a key fob transmitter. The receiver will function in either hot or cold temperatures while the transmitter will operate at moderate temperatures.

Suppose the receiver will run at -15°C. A typical crystal will add 11.5 ppm error due to the temperature drift. Thus, the receiver crystal error will be:

EQUATION 13: ADDITION PPM ERROR AT -15 DEGREES CELSIUS

$$\varepsilon = 30\ ppm + 11.5\ ppm$$

The total deviation for a month period will be:

EQUATION 14: WORST-CASE TIMER ERROR CALCULATION FOR ONE MONTH PERIOD, TAKING INTO ACCOUNT THE ADDITIONAL ERROR DUE TO TEMPERATURE

$$60s * 60\ min * 24\ hours * 31\ days * 41.5\ ppm \cong 111.15\ seconds$$

These parameters are different with different crystals and manufacturers. The user needs to consult the crystal specifications in order to get the exact initial tolerance and temperature drift for one particular crystal. Also, some manufacturers are shipping crystal oscillators that have been individually measured before shipping.

4.1.4 USING THE WDT PERIOD

The Watchdog Timer runs on a separate internal oscillator. Its typical time-out period is specified as 16 ms typical (when using 1:512 prescaler) with a possible error of up to ±25%. In one month, this gives us a maximum deviation of:

EQUATION 15: WORST-CASE TIMER ERROR CALCULATION FOR ONE MONTH PERIOD

$$60s * 60\ min * 24\ hours * 31\ days * 25\% = 669{,}600\ seconds$$

The above calculations are worst-case scenarios. These numbers are showing much larger tolerances compared to the precision of the crystal driven timers. While these numbers may seem very big, they are, however, fairly predictable. It is no doubt that the precision is lower, but for a number of cost-effective applications, the WDT time-keeping method is perfectly usable.

4.2 Receiver Time Source Examples

4.2.1 TMR1 PERIPHERAL WITH 32.768 kHz OSCILLATOR

The receiver can use a similar timer driven by a 32.768 kHz crystal (if not the same part).

4.2.2 RTCC

The Ultimate KEELOQ technology system depends on the constant synchronization between the timers at both the encoding and decoding end; however, a power loss can occur at both ends.

On the transmitter side, a low battery condition or battery replacement operation can interrupt this synchronization. Resynchronization is achieved, either automatically or manually, by re-learning an encoder.

On the receiver side, a power loss is something more serious. Because the receiver needs to be synchronized with a number of remote controls, manually resynchronizing all remotes is not feasible. The best option for this is the use of an external battery-powered real time clock. This way the receiver can easily recover from a power loss and automatically resynchronize.

5.0 SUMMARY COMPARISON OF SYSTEMS

This application note describes the three currently available KEELOQ technology implementations: Classic KEELOQ technology, Advanced KEELOQ technology and Ultimate KEELOQ technology. These three KEELOQ technology implementations can cover a wide range of security applications. The designer needs to have good understanding of the application's security requirements and choose the best suited KEELOQ technology implementation. Every "step" in KEELOQ security not only adds a new level of security but also a new level of complexity and a new level of hardware requirements.

Classic KEELOQ technology is the basic level of KEELOQ security. It provides a good level of security while being cost-effective. Advanced KEELOQ technology adds more security by using a stronger encryption algorithm and a longer encryption key. Ultimate KEELOQ technology provides the strongest security level, by adding a very precise synchronization mechanism, using data packets that are valid only for a very narrow time frame, also providing data integrity and authentication.

NOTES:

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.

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE**.** Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights.

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
═ ISO/TS 16949 ═

Trademarks

The Microchip name and logo, the Microchip logo, dsPIC, FlashFlex, KEELOQ, KEELOQ logo, MPLAB, PIC, PICmicro, PICSTART, PIC^{32} logo, rfPIC, SST, SST Logo, SuperFlash and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

FilterLab, Hampshire, HI-TECH C, Linear Active Thermistor, MTP, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

Analog-for-the-Digital Age, Application Maestro, BodyCom, chipKIT, chipKIT logo, CodeGuard, dsPICDEM, dsPICDEM.net, dsPICworks, dsSPEAK, ECAN, ECONOMONITOR, FanSense, HI-TIDE, In-Circuit Serial Programming, ICSP, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mTouch, Omniscient Code Generation, PICC, PICC-18, PICDEM, PICDEM.net, PICkit, PICtail, REAL ICE, rfLAB, Select Mode, SQI, Serial Quad I/O, Total Endurance, TSHARC, UniWinDriver, WiperLock, ZENA and Z-Scale are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

GestIC and ULPP are registered trademarks of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

♻ Printed on recycled paper.

ISBN: 978-1-63276-198-9

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

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

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

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

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110

Canada - Toronto
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2943-5100
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Hangzhou
Tel: 86-571-8792-8115
Fax: 86-571-8792-8116

China - Hong Kong SAR
Tel: 852-2943-5100
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8864-2200
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-3019-1500

Japan - Osaka
Tel: 81-6-6152-7160
Fax: 81-6-6152-9310

Japan - Tokyo
Tel: 81-3-6880- 3770
Fax: 81-3-6880-3771

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-5778-366
Fax: 886-3-5770-955

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Dusseldorf
Tel: 49-2129-3766400

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Pforzheim
Tel: 49-7231-424750

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Venice
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Poland - Warsaw
Tel: 48-22-3325737

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820

03/25/14