English

MCR-300/UART

PowerCode Receiver Interface Module

Visonic®

User Guide

1. INTRODUCTION

The MCR-300/UART module is a PowerCode receiver interface module designed to communicate with Visonic PowerCode / CodeSecure wireless devices. The module includes a super-heterodyne receiver module, specifically for digital data transfer on UHF radio channels. Its main application is as an RF interface unit used in security systems that communicates digital codes and reports. The receiver features serial data output at CMOS levels, which may be applied to a decoder or directly to a micro-processor unit.

The Module decodes PowerCode & CodeSecure wireless messages and transfers them into a serial bit stream as defined by the receiver protocol description.

The module includes two integral antennas for diversity reception, allowing high performance reception, overcoming "in-band" interference.

Mechanical support and electrical connections to the MCR-300/UART are obtained by mounting the module on a 5-pin header seated on the host motherboard. The header pins are connected to a panel.

2. SPECIFICATIONS

Receiver Type: Single-channel, UHF super-heterodyne receiver.

Frequency: 868.95 MHz

Bandwidth: 400 kHz @ -3dB points

Data Rate: Up to 1 kbps NRZ.

Data Output Levels: 0V (LOW) and 5V (HIGH).

Baud rate: 9600

Parity bit: None

Data bit: 8

Stop bit: 1

UART interface

2 Integral Antennas diversity reception allowing high performance reception, overcoming "in-band" interference. Length: 80mm

Supply Voltage: 5 VDC ±5%.

Current Consumption: 15 mA @ 5 VDC.

2 MGC-Manual Control Gain:

- MGC - High "5V" - Sensitivity attenuation 30dB.
- MGC - High impedance - Normal Sensitivity

Note: *Do not connect MGC to GND*

Operating Temperatures: 0°C to 49°C (32°F to 120°F).

Dimensions: 52.5 x 51 x 12 mm

Compliance with Standards: Complies with EN 301 489-3 V1.2.1 (2000-08), EN 300 220-1 (1999) and EN 50131-1 Grade 2, Class II requirements.

Note: *A sample disc can be obtained on email request.*

ATTENTION
OBSERVE PRECAUTIONS FOR HANDLING ELECTROSTATIC SENSITIVE DEVICES

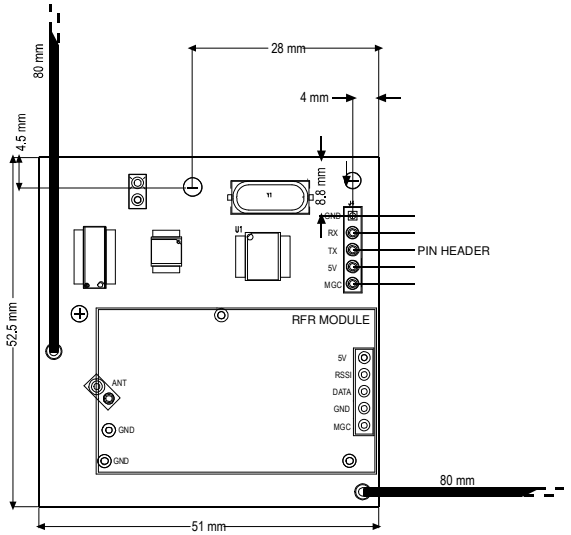
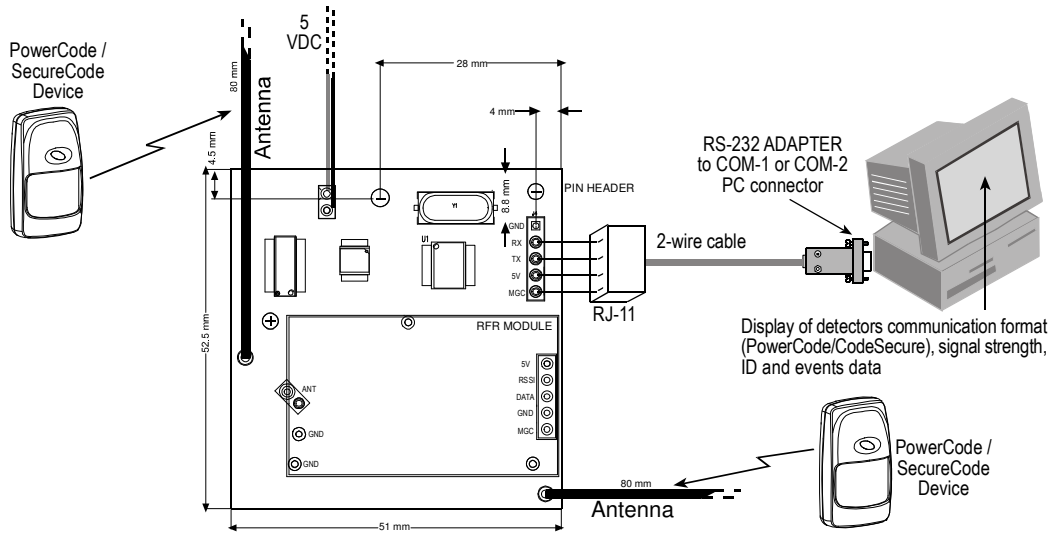


Figure 1. *Top View of PCB and Electrical Connections*

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

3. WIRING AND SETTINGS



Note: *Make sure that com ports 1 and 2 of your computer are not being used by another application.*

Figure 2. *Functional Diagram*

4. DEMONSTRATION BOARD

4.1 The System and RF Communication

The MCR-300/UART is designed to be integrated into your control panel. The Module consists of a microprocessor and several other components. To aid in the understanding of the structure and content of messages a demonstration board was set up together with a unique computer software program. The demonstration board can be connected to the computer's COMM port for viewing messages received from the RF receiver. These messages appear in the same format as the messages sent by the module to the control panel.

For a general understanding, we will examine the structure of the received RF message.

Receiving RF message structure

A receiving RF message is sent only if two such messages are received with true checksum (Power code) or with true lowest 10 bits of ID and function key (CodeSecure) in the same packet of messages.

RF message structure for PowerCode

Power code message	36 bits
ID-24bits	3 bytes
DATA	1 byte
Check sum	0.5 byte

CodeSecure message (66 bits):

Encrypted code	4 bytes
ID-28bits	3.5 bytes
Function Key	0.5 byte
Last byte (9^{th})	RL

The RS232 Message Structure (10 or 3 bytes)

The RS232 message is sent at a rate of 9.6 KBaud.

There are two types of messages sent by the Receiver Module:

- Data message
- Control message

The Data message contains the data of a RF message received from the RF receiver.

The Control message contains data on jamming events and supervision data to support the communication link between the Receiver Module and the Control Panel.

Data message format (10 bytes):

Start '>' 3E(H)	1 byte
Status	1 byte
RF Message	7 bytes
Check Sum	1 byte

Control message format (3 bytes):

Start '>' 3E(H)	1 byte
Status	1 byte
Check Sum	1 byte

Both types of messages start with a Start byte of value 0x3E, and end with a Checksum byte. The messages also have a Status byte. The Data message includes the contents of the received RF message.

RS232 dialog between the Receiver Module and the Control Panel.

A message will be sent a maximum of 3 times. After each transmission the module waits for acknowledgement from the control panel. If an acknowledge signal/message is not received within 50 ms, the same message will be sent again.

The Receiver Module sends a Supervision message (using a Control message) every minute. Any Data message or Control message, successfully sent, is also considered a supervision message. Timer of supervision at the Receiver Module is cleared after every message that is sent.

An acknowledge message will be sent by the Control Panel to the Receiver Module after every message sent by the Receiver Module. This includes data messages and control messages. The acknowledged message will be of the character '<' = 0x3C.

4.2 Status Byte Structure (control message)

Bit	Name	Value	Meaning
0,1	Jamming level	00	No jamming detected
		01	USA jamming level
		10	European standard jamming level
		11	---
2,3	Not used	0	Constantly 0
4-7	Message type	0000	Not used
		0001	Supervision message from Module to Control Panel (not RF supervision)
		0010	Not used
		0011	PowerCode message includes jamming (if detected)
		0100	CodeSecure message includes jamming (if detected)

4.3 The RF Message PowerCode Structure (7 bytes)

ID-24bits 3 bytes	DATA 1 byte	DATA 1 byte	xxxx 2 bytes

<----- Sending direction

Contents of DATA byte for PowerCode

Bit	Name	Value	Meaning
0	Tamper	1	Tamper event
1	Alarm	1	Alarm event
2	Low Battery	1	Low battery at transmitter
3	Working bit		
		0	Else
4	Restore	1	Transmitter has a restore capability, e.g. Magnet
		0	Transmitter with no restore, e.g. PIR detector
5	Supervise	1	Supervised transmitter
		0	Non-supervised transmitter, e.g. Panic button
6	SpiderNet	1	Transmitter works in a Spider system (Not relevant)
		0	A regular transmitter, not in a Spider system
7	Repeater	1	The transmitter is a Repeater. Displays messages received from a repeater in the system.
		0	Any other transmitter

Contents of DATA1 byte for PowerCode:

Bit	Name	Value	Meaning
0,1	Quality of RF signal of last message received	00	Poor
		01	Good
		10	Strong
		11	Not used
2-7	Not used	0	All bits are constantly 0

RF message structure for CodeSecure (7 bytes) - Keyfob

ID-28bits 4 bytes					DATA 1 byte		Sync counter 2 bytes	
1 byte LSB	2 bytes	3 bytes	4 MSB bits		7	0	1 LSB byte	2 MSB bytes
			000 0	xxx x	FFF F	0LQ Q		

<----- Sending direction

Contents of DATA byte for CodeSecure

Bit	Name	Value	Meaning
0,1	Quality of RF signal of last message received	00	Poor
		01	Good
		10	Strong
		11	---
2	Low Battery	1	Low battery at transmitter
3	Not used	0	Constantly 0
4-7	Function key / button on transmitter - F1, F2, F3, F4.	1xxx	Button 1 pressed, bit 4

	Two or more buttons may be pressed simultaneously, e.g. 1010 = 1, 3 pressed.		
		x1xx	Button 2 pressed, bit 5
		xx1x	Button 3 pressed, bit 6
		xxx1	Button 4 pressed, bit 7

The Jamming Bits

There are two standards for jamming decision that are implemented in the system: European standard and American (USA) standard. The two differ slightly.

The common part of those standards is:

1. For every second, a **jamming state** is detected if during 18% of a second the disturbances are larger than a predefined threshold.
2. **Jamming event** is declared if the jamming state persists for 30 or more seconds of the minute.
   The difference between the USA and European standards are as follows:
   - USA standard requests continuous 30 or more seconds of jamming state.
   - European standard requests any 30 or more seconds of jamming state during one minute.

   Clearly, not every jamming event defined as European standard is considered a jamming event according to USA standard.

CodeSecure Implementation

CodeSecure implements the KELOQ code hopping technology to make each transmission by an encoder unique. The encoder transmissions are comprised of two parts. The first part changes each time the encoder is activated and is called the "hopping code". The second part is the serial number of the encoder (ID), recognizable to a decoder.

The hopping code contains function information, a discrimination value and a synchronization counter. An encryption algorithm encrypts this information before being transmitted. The encryption algorithm uses a 64-bit encryption key. If one bit in the data that is encrypted changes, the result is that an average of half of the bits in the output will change. As a result, the hopping code changes dramatically for each transmission and cannot be predicted.

The transmitted word contains a 16-bit **synchronization counter**. The counter is incremented every time the encoder is activated.

The synchronization information is used at the decoder to determine whether a transmission is valid, or a repetition of a previous transmission is being sent. When a following transmission is received from the same transmitter it is possible to verify whether the transmission is valid. Previous codes are rejected to safeguard "code grabbers". The range of the synchronization counter is 65,536. Each transmission, for example, a button press, generates a new synchronization number, one out of the 65,356.

Implementation Guidelines

Storing serial numbers - The synchronization counter value is stored in EEPROM of the control panel every time a valid transmission is received from a particular encoder. **It is highly recommended to keep two copies of the synchronization counter in two different EEPROM locations**. This is because that in the event of a power failure during an EEPROM write, a corrupted counter value would be read when the control panel is later powered up, resulting in encoder transmissions erroneously being discarded as invalid.

The encoder's serial number is transmitted every time a button is pressed. The serial number is transmitted unencrypted as part of the transmission. A serial number is used at the Receiver Module to check message correction after message decryption, and at the control panel to verify whether transmitter is valid. **Serial numbers of every valid transmitter must be stored in EEPROM of the control panel**.

Algorithm of synchronization counter control

Conditions must be established where the transmitter is pressed while out of valid range of the RF Receiver. Allowing two "synchronization windows" achieves this:

- The open window
- The resynchronization window

The **open window** is a reception of a transmission where the synchronization counter is 1 to 16 higher than the previous counter value received. The reception of such a signal will result in an immediate counter update by the control panel program and the appropriate outputs being activated.

If the transmitter is pressed more than 16 times out of range of the receiver, resynchronization needs to be performed. The **resynchronization window** is half of the total counter range, 32K numbers. During resynchronization, the control panel program waits for two consecutive transmissions from the encoder before resynchronization occurs and the resynchronized counters are updated in the EEPROM of the control panel. When the control panel receives a transmission with a synchronization counter value more than 16 above the stored counter value and less than 32,768 counts above the stored value, the control panel temporarily stores the value of the synchronization counter received. If the next transmission received has a synchronization counter value of one above the previous sent, the control panel resynchronizes on the last transmission received and activates the appropriate outputs.

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

5. OPERATION

5.1 Viewing all Detector IDs

Note: *Use a MCR-300/UART unit whose receiving frequency is identical to the frequency of the detectors.*

The following steps are performed for checking detector IDs within the system.

1. Insert the CD-ROM into the CD-ROM drive.
2. Copy the contents of the CD-ROM into a new folder on your PC.
3. From your PC, double-click the MCW_LINK_DOS.exe file.
4. Press 1 or 2 on your keyboard to establish which COM port is being used; a window displays a list of all the registered detectors within the system and their IDs, as shown in Figure 2.
5. To view a specific detector ID you should initiate an event, for example, alarm or tamper (a tamper event is initiated by opening and closing the cover).
6. Write down the ID (6 characters, for example, F384B3).
7. Click X on the top right corner of the window to close the window.
8. A new window will open; click End Now.

   Notes:

   a) When receiving and viewing messages on your screen the software creates a new file in the directory you already opened containing the MCW_LINK_DOS.exe file and ID_TABLE.txt file. This new file will contain a name that includes the date of the received messages, for example, THUSEP23.txt (day/month/date.txt). This enables the computer to automatically create a log file of all received messages. Every day the computer automatically opens a new file with the date included in the file name.

   b) You can convert the .txt data file into an Excel data sheet (.xls) by clicking File→Open then launching the daily file from the directory to which it was saved. Follow the remainder of the instructions of the Text Import Wizard.

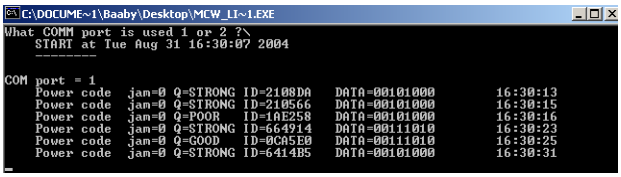


Figure 2. *All Detector ID window*

5.2 PowerCode - Viewing Specific Detector IDs

To view specific detector IDs, you need to enroll the required detectors by filling a simple .txt file to provide details of the detector ID.

1. From your PC, double-click the ID_TABLE.txt file.
   Note: *If the file opens as Read-only, from Windows Explorer right-click the file, select Properties, then click the General tab. Deselect the Read-Only checkbox, then click OK.*
2. Enter the ID of the detector; enter each ID on a separate row.
3. Save the ID_TABLE.txt file using the same file name (from the File menu, click Save).
4. Click X on the top right corner of the window to close the ID_TABLE.txt window.
5. Double-click the MCW_LINK_DOS.exe file.
6. Press 1 or 2 on your keyboard to establish which COM port is being used; a window displays a list of all the enrolled detectors and their IDs, as shown in Figure 3.

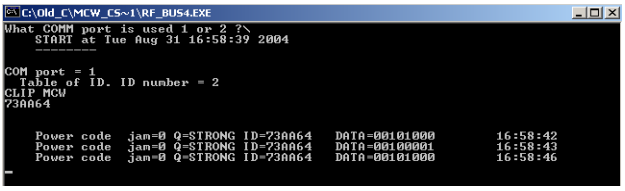


Figure 3. *Specific Detector ID window*

PowerCode Message Definitions:

Display field	Name	Definition
1	Jamming	0 = No jamming E = European STD jamming level U = USA STD jamming level
2	Quality of RF signal	POOR / GOOD / STRONG
3	ID	The detector's ID (6 characters)
4	Data	7 6 5 4 3 2 1 0 (see Para.4.3)
5	Time of event	hh:mm:ss (24 h format)

7. The system now begins to monitor the enrolled detectors. The window will display the detectors you selected as shown in Figure 3.

Note: *The PowerCode Message Definitions table explains how to read the data. The Definition of DATA bits in a PowerCode Message table explains each bit of the DATA field in a PowerCode message.*

8. Click X on the top right corner of the window to end the monitoring and to close the window.

9. A new window will open; click End Now.

Definition of DATA bits in a PowerCode Message:

Bit	Name	Value	Meaning
0	Tamper	1	Tamper event
1	Alarm	1	Alarm event
2	Low Battery	1	Low battery at transmitter
3	Working bit		
		0	Else
4	Restore	1	Transmitter has a restore capability, e.g. Magnet
		0	Transmitter with no restore, e.g. PIR detector
5	Supervise	1	Supervised transmitter
		0	Non-supervised transmitter, e.g. Panic button
6	SpiderNet	1	Transmitter works in a Spider system (Not relevant)
		0	A regular transmitter, not in a Spider system
7	Repeater	1	The transmitter is a Repeater. Displays messages received from a repeater in the system.
		0	Any other transmitter

5.3 CodeSecure - Viewing Specific Keyfob IDs

To view specific keyfob IDs, you need to enroll the required keyfobs by filling a simple .txt file to provide details of the keyfob ID. To perform this, follow the instructions in section 4.2.

Figure 4 displays the messages sent by a keyfob, where all four keyfob buttons were pressed consecutively.

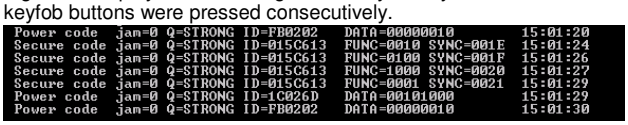


Figure 4. *Specific Keyfob ID window*

The CodeSecure Messages table provides the definition of each field in a keyfob message.

CodeSecure Messages:

Display field	Name	Definition
1	Jamming	0 = No jamming E = European standard jamming U = USA jamming
2	Quality of RF signal	POOR / GOOD / STRONG
3	ID	7 character ID, for example, 015C613
3	FUNC	Button number; the 4 buttons have code numbers 0010, 0100, 1000, 0001
4	SYNC	Transmission serial number
6	Time of event	hh:mm:ss (24 h format)

W.E.E.E. Product Recycling Declaration

For information regarding the recycling of this product you must contact the company from which you orignially purchased it. If you are discarding this product and not returning it for repair then you must ensure that it is returned as identified by your supplier. This product is not to be thrown away with everyday waste.

Directive 2002/96/EC Waste Electrical and Electronic Equipment.

VISONIC LTD. (ISRAEL): P.O.B 22020 TEL-AVIV 61220 ISRAEL. PHONE: (972-3) 645-6789, FAX: (972-3) 645-6788
VISONIC INC. (U.S.A.): 65 WEST DUDLEY TOWN ROAD, BLOOMFIELD CT 06002-1376. PHONE: (860) 243-0833, (800) 223-0020 FAX: (860) 242-8094
VISONIC LTD. (UK): FRASER ROAD, PRIORY BUSINESS PARK, BEDFORD MK44 3WH. PHONE: (0870) 730-0800 FAX: (0870) 730-0801
INTERNET: WWW.VISONIC.COM

 MCR-300/UART DE3140U (REV. 0, 11/05)

MADE IN ISRAEL