Cello-AR Integration Manual

Cellocator Division
Pointer Telocation Ltd.

Proprietary and Confidential

Version 1.2

Revised and Updated: January 20, 2013

POINTER

Pointer Telocation Ltd. 14 Hamelacha St., Rosh Ha'ayin 48091, Israel • Tel: 972-3-5723111 • Fax: 972-3-5723100 • www.pointer.com

Legal Notices

IMPORTANT

1. All legal terms and safety and operating instructions should be read thoroughly before the product accompanying this document is installed and operated.
2. This document should be retained for future reference.
3. Attachments, accessories or peripheral devices not supplied or recommended in writing by Pointer Telocation Ltd. may be hazardous and/or may cause damage to the product and should not, in any circumstances, be used or combined with the product.

General

The product accompanying this document is not designated for and should not be used in life support appliances, devices, machines or other systems of any sort where any malfunction of the product can reasonably be expected to result in injury or death. Customers of Pointer Telocation Ltd. using, integrating, and/or selling the product for use in such applications do so at their own risk and agree to fully indemnify Pointer Telocation Ltd. for any resulting loss or damages.

Warranty Exceptions and Disclaimers

Pointer Telocation Ltd. shall bear no responsibility and shall have no obligation under the foregoing limited warranty for any damages resulting from normal wear and tear, the cost of obtaining substitute products, or any defect that is (i) discovered by purchaser during the warranty period but purchaser does not notify Pointer Telocation Ltd. until after the end of the warranty period, (ii) caused by any accident, force majeure, misuse, abuse, handling or testing, improper installation or unauthorized repair or modification of the product, (iii) caused by use of any software not supplied by Pointer Telocation Ltd., or by use of the product other than in accordance with its documentation, or (iv) the result of electrostatic discharge, electrical surge, fire, flood or similar causes. Unless otherwise provided in a written agreement between the purchaser and Pointer Telocation Ltd., the purchaser shall be solely responsible for the proper configuration, testing and verification of the product prior to deployment in the field.

POINTER TELOCATION LTD.'S SOLE RESPONSIBILITY AND PURCHASER'S SOLE REMEDY UNDER THIS LIMITED WARRANTY SHALL BE TO REPAIR OR REPLACE THE PRODUCT HARDWARE, SOFTWARE OR SOFTWARE MEDIA (OR IF REPAIR OR REPLACEMENT IS NOT POSSIBLE, OBTAIN A REFUND OF THE PURCHASE PRICE) AS PROVIDED ABOVE. POINTER TELOCATION LTD. EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY PERFORMANCE AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL POINTER TELOCATION LTD. BE LIABLE FOR ANY INDIRECT, SPECIAL, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OR INTERRUPTION OF USE, DATA, REVENUES OR PROFITS) RESULTING FROM A BREACH OF THIS WARRANTY OR BASED ON ANY OTHER LEGAL THEORY, EVEN IF POINTER TELOCATION LTD. HAS BEEN ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.

Intellectual Property

Table of Contents

1 Introduction

This document summarizes the changes in programming and the OTA communication of the Cello-AR system, compared with the Cello-F.

This document does not describe the basic functionality of the Cello-AR Security System and installation aspects. This functionality is described in documents listed in the *References* section below.

Note: the wireless immobilizer and the CLOCK and LOCK (C&L) feature have not been implemented yet and information provided regarding them should be regarded as infrastructure for future implementation only.

1.1 Revision History

Version	Date	Description
1.0	September 9, 2012	Initial version
1.1	October 30, 2012	Updates and disclaimers for GA release
1.2	January 20,2013	Add disable pairing bit on byte 1710 Remove installation diagram from overview section

1.2 References

No.	Document Name	Remark
1	Cello-AR security product overview	
2	Programming Manual for Cellocator Cello	
3	Cellocator Wireless Communication Protocol	
4	Serial Interfaces Specification	

2 General

2.1 Overview

The Cello-AR Security system provides anti-theft security capabilities (in addition to the regular Fleet management) based on:

- Driver identification and authentication.
- Robust and smart immobilizing system with a redundancy option.
- Theft or tamper attempts detection and OTA reporting to the control center (early alert).
- OTA diagnostics and control, including FOTA upgrade.
- Security diagnostic capabilities.
- Flexibility through programmable parameter settings sent via the control center.

The Cello-AR system supports the following features:

- Security states: armed, disarmed, standby, garage / service, keypad locked. The states also include manual and automatic procedures for entering and exiting the states.
- Disarming the system via user code, master code, and emergency disarming using the ignition switch.
- Changing the user code.
- Identifying, assigning and removing the assignment of the immobilizing devices.
- OTA communication with the control center for event reporting, parameter programming and the receiving of commands.
- Identification and authentication method based on user code, and authentication code (Multi-Code).
- CLOCK and LOCK (C&L) including separate parameters for each day of the week.
- ECall and BCall using Cellocator Hands Free.

The Cello-AR Security system consists of a keypad, immobilizers and the Cello-AR unit. The smart immobilizers utilize relay to deactivate the vehicle engine and maintain wire or wireless communication with the AR Keypad. The AR Keypad, via which the driver/technician interacts with the system, controls the immobilizers. They AR Keypad is connected to the Cello-AR unit, which controls the keypad and communicates with the control center application.

In order to provide these capabilities the following components are needed:

- Keypad for driver authentication with visual and audible indication devices (e.g. LED, buzzer).
- At least one immobilizing device.
- A Cello-AR unit.

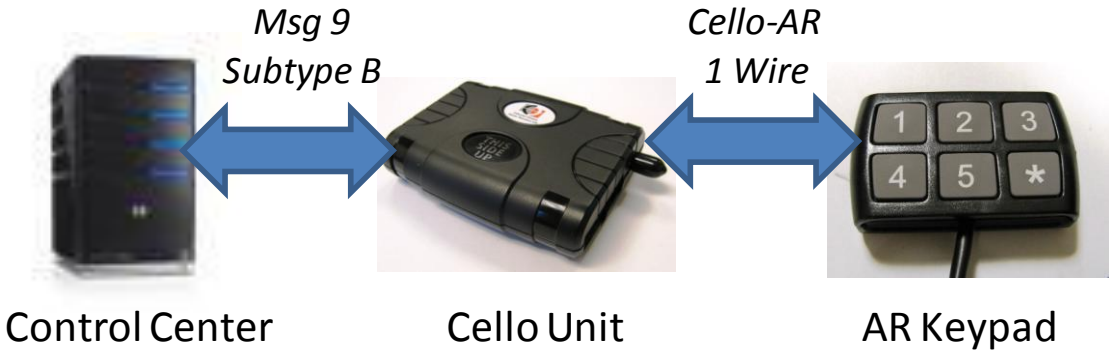
For further details you are welcome to review the Cello-AR security product overview

2.2 Delays and Multi-command Management

The AR system sends acknowledgement for each received command, for the special AR capabilities, to the control center application as a payload of Message type 9 subdata type B.

Internal system communication might delay events reporting and commands executing. Events reporting might be delayed up to several hundreds of milliseconds while commands executing might be delayed up to several seconds.

Further delay, due to internal communication, is expected in case of multiple commands sent toward the system. This is caused due to the acknowledge mechanism utilized in the internal communication.



3 Configuration Aspects

3.1 New Parameters

The following new parameters were added to the Cello-AR security system.

3.1.1 *AR Keypad Controlling Bitmask*

Address: 1709-1710

Keypad disconnection Disable (0) Enable (1)			Wrong keypad detection Disable (0) Enable (1)			AR keypad MSG type 9 data source (Log or Direct) Log (0) Real time (1)	Enable AR keypad Disable (0) Enable (1)
Log	Distress	Alarm Cadence	Log	Distress	Alarm Cadence		
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Address: 1710

Unused		Disable pairing Disable (1) Enable (0)	Msg Type 0 Ack Reply Enable Disable (0) Enable (1)	Activate Alarm Cadence upon Hot Wiring detection Disable (0) Enable (1)	Malfunction report Disable (0) Enable (1)		Enable Forwarding data from keypad to Serial Port Disable (0) Enable (1)
					Log	Distress	
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

3.1.2 *Alarm Cadence outputs bitmask*

Address: 450

Unused			Blinkers	Unused			Siren
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

3.1.3 *Alarm Cadence duration and cycles*

Address: 1712

Reserved				Number of cycles			
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Address: 1713

On Time of Alarm Cadence activation (3 Seconds/bit)				Off time (between activations, 3 seconds/bit)			
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

3.1.4 *ECALL Voice Call Destination number*

Addresses: 273-282

Stores the default target address used by the unit to establish an ECALL (in the same format as the Default voice destination number used in the standard Cello-F unit).

Default value: NULL

3.1.5 *BCALL Call Destination number*

Addresses: 167 – 176

Stores the default target address used by the unit to establish a BCALL (in the same format as the ECALL voice call destination number).

Default value: NULL

3.2 Description of the Parameters

3.2.1 *Enable AR Keypad*

If this bit is enabled (1), the system will operate the Cello AR 1-Wire interface protocol over its Dallas port and therefore:

- Cancels any driver ID internal logic, including reminders.
- Allows communication of security information with the control center application (using OTA Msg type 9, sub-data 0xB).
- Allows operation of the security special features and capabilities.

Default: 0 – Disabled.

3.2.2 *OTA data delivery method*

This bit defines the OTA delivery method of messages type 9, with the security information.

- 0 – will cause the unit to deliver this message as a logged event using the same rules (same numerator sequence, requires acknowledge).
- 1 – will cause the unit to deliver it as a real time event. In this case the ACK is unnecessary; the message will be delivered by the first available communication transport.

Default: 0 – Disabled.

3.2.3 *Enable Alarm Cadence/logged Event/Distress upon wrong keypad ID detection*

If a corresponding bit is enabled, and the pairing procedure was accomplished, the unit will activate an Alarm Cadence (refer to the *Alarm Cadence* section), and generate an event or distress upon detection of an invalid (not paired) keypad.

The OTA event/distress message is type 0 with TR 91, STR 11.

The unit will repeat event/distress/Alarm Cadence after the pairing procedure is repeated.

Default: 000 – All Disabled.

3.2.4 *Enable Alarm Cadence/logged Event / Distress upon keypad disconnection detection*

If this bit is enabled, and the pairing procedure was accomplished, the unit activates an Alarm Cadence, and generates an event or distress 16 seconds after the last keypad ID detection.

If Pairing is enabled:

The unit will send OTA event/distress message type 0 with TR 201, STR 0. The Com. Status in byte 33 of OTA Msg type 0 will contain 1 (Communication Loss or pairing Failed).

If pairing is disabled:

The unit will send OTA event/distress message type 0 with TR 201, STR 0. The Com. Status in byte 33 of OTA Msg type 0 will contain 1 (Communication Loss only).

Default: 000 – All Disabled.

3.2.5 *Enable Forwarding data from keypad to Serial Port*

If this bit is enabled (1), any OTA Messages Type 9, Sub-Data Type B from AR system (except message type 0x88) will be sent also to the serial port of the Cello-AR , otherwise only to the wireless channel.

Default: 0 – Disabled.

3.2.6 *Enable Malfunction / Alert report (Event/Distress)*

If those bits are enabled upon detection of the corresponding event, the system will trigger an OTA update event/distress with transmission reason 91 and a specific transmission reason, as listed in the table below.

STR	Description

STR	Description
0	Keypad Undefined Failure
1	Immobilizer Device Wires Disconnection
2	Keypad Locked
3	Relay Malfunction
4	Ignition Wire Disconnected
5	Starter Signal Detection
6	Starter Malfunction
7	Hotwiring Detection
8	Primary Cut Unit Failure
9	Secondary Cut Unit Failure
10	Wrong Keypad ID Detected
11	Pairing Accomplished
12	Keypad Flash Failed
13	Alarm Cadence Activated by Keypad
14	Alarm Cadence Deactivated by Keypad
128*	ECALL Initiated
129*	BCALL Initiated

* This STR is sent as single real time event before call initiation, irrespective of the status of the bits.

3.2.7 *Activate Alarm Cadence upon Hotwiring detection*

If this bit is enabled the unit will auto-activate Alarm Cadence upon detection of Hot Wiring (engine starts on armed state).

Default: 0 – Disabled.

3.2.8 *Msg Type 0 Ack reply Enable*

If enabled, the unit will generate an active ACK (Message type 0, Reply) to OTA Messages type 9, sub-type B.

Default: 0 – Disabled.

3.2.9 *Disable Pairing*

If this bit is enabled the Cello-AR unit will bypass pairing process with the keyboard.

Default: 0 – Pairing Enabled.

3.3 Alarm Cadence

Alarm Cadence is an activation of selected outputs for a session of sequential pulses, used for visual and audio alarm notification. Alarm Cadence can be activated by an OTA command, or by internal logic further to the detection of a wrong keypad ID or keypad disconnection (as per the configuration described above).

3.3.1 *Use Siren for Alarm Cadence*

If this bit is enabled the unit will utilize the Siren output for Alarm Cadence pulses.

Default: 0 – Disabled.

3.3.2 *Use Blinkers for Alarm Cadence*

If this bit is enabled the unit will utilize the Blinkers output for Alarm Cadence pulses.

Default: 0 – Disabled.

3.3.3 *Alarm Cadence: Number of cycles*

This parameter defines the number of activations of selected outputs during Alarm Cadence.

Default: 0.

3.3.4 *Alarm Cadence: Activation Time*

This parameter defines the activation time of selected outputs during Alarm Cadence.

Default: 0 (resolution of 3 seconds/bit).

3.3.5 *Alarm Cadence: Time between activations*

This parameter defines the time between activations of selected outputs during Alarm Cadence.

Default: 0 (resolution of 3 seconds/bit).

4 Data Traffic from AR System to Control Center

4.1 Cello-AR status reporting in Msg. type 0

The system handles the security events and status changes and continually reports them in the type 0 OTA messages from the Cello unit as follows:

- Continuous of the AR security system status is reporting in message type 0 in Dallas field (bytes 33-38)
- malfunction/alarms/disconnection or voice call requests cause the unit to generate a position message (Type 0, TR91 (dec) with corresponding value in a STR field)
- Reception of the user code causes the unit to generate a position message (Type 0, TR46 (dec) with value 1 in a STR field).

4.1.1 *Communication Control byte*

When the AR keypad is enabled in programming, the unit sets bits 4-5 of byte 10 of OTA Message type 0 to '10' in all the messages except Driver Authentication Update (TR46) and Wake Up (TR202).

The **"Bytes 33-38 assignment (Dallas, PSP or other)"** bits define the data type, provided in bytes 33-38 of this message, according to the table below.

Bit 5	Bit 4	Description
0	0	Backward compatibility mode (to FW 27c and below), Driver ID (Dallas field)
0	1	PSP mode is enabled, external Alarm device data is transmitted in bytes 33-38
1	0	AR keypad support is enabled; AR security data is transmitted in bytes 33-38
1	1	Reserved for future use

4.1.2 *Dallas bytes 33-38*

Reserved			Latest AR security Status		Com. Status (see below)
Nibbles 6-11			Nibbles 1-5		Nibble 0
Byte 38	Byte 37	Byte 36	Byte 35	Byte 34	Byte 33

bytes 33-38 contains the following information if Bits 4 and 5 of Communication Control byte are set to AR keypad support.

4.1.3 *Com. Status Table (low nibble of byte 33)*

Value	Description
0	AR keypad status in following 5 nibbles
1	If Pairing is enabled (Address 1710 bit 5) The unit will send OTA event/distress message type 0 with TR 201, STR 0. The Com. Status in byte 33 of OTA Msg type 0 will contain 1 (Communication Loss or pairing Failed). If pairing is disabled (Address 1710 bit 5): The unit will send OTA event/distress message type 0 with TR 201, STR 0. The Com. Status in byte 33 of OTA Msg type 0 will contain 1 (Communication Loss only).
2-7	Reserved

4.1.4 *Latest AR system Status*

The value of the following bits is updated every time when:

- The code is received
- Operational security state changed
- Ignition Change detected

D19	D18	D17	D16	D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
High Nibble				Low Nibble				High Nibble				Low Nibble				High Nibble			
Byte 35								Byte 34								Byte 33 (high nibble)			

Bit	Name	Description
D0	Door (from Cello unit)	Contains Logical Door Input (of Cello unit) status (inverted and filtered)
D1	Volume Meter	
D2		
D3	Ignition	AR keypad Ignition input status
D4	Alarm Armed ON	Represents Immobilizer bit received from keypad. Same as D8.

Bit	Name	Description
D5	Not available, sent as zero	
D6		
D7		
D8	Immobilizer Armed ON	Represents Immobilizer bit received from keypad. Same as D4.
D9	Not available, sent as zero	
D10	Hot Wiring	Set on Hotwiring detected, reset upon entrance of Operational State 0 or 1
D11	Service	Set when Operational State = 4 Reset in any other Operational State
D12	Keypad Wrong Code	Updated on entering access code is: Set when bit 3 or bit 4 of code recognition status byte is 1 Reset when both bit 3 and bit 4 of code recognition status byte are 0
D13-D19	Zeros	

4.1.5 *Code Update messages*

When the user enters an access code using the AR keypad, the Cello unit triggers a Driver Authorization update event/distress (TR46, STR 1), as per settings in the programming bit on address 0x7B, bit 1 (event) and 0x1E4, Bit 1 (distress).

The message contains the received code and recognition status. Bits 4 and 5 of the Communication Control byte contain zeros.

Code Recognition Status (8 bits)	Spare	Received Code (32 bits)
Byte 38	Byte 37	Byte 33-36

Code Recognition Status (Byte 38)

Reserved	Immobilizer Status 0 – off 1- on	Ignition Status 0 – off 1- on	Authentication (multi-code) Code status 0- OK 1- Wrong	Code status 0- OK 1- Wrong	Code type 0- Standard Authentication 1- C&L 2- 7 - reserved 3-		
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Received Code (Bytes 33-36)

Master code, only in case of reply to access code request, otherwise sent as zeros				LSB char of the code	3rd char of the code	2nd char of the code	MSB char of the code
LSB char of Master code	3rd char of the Master code	2nd char of the Master code	MSB char of Master code				
Nibble 8	Nibble 7	Nibble 6	Nibble 5	Nibble 4	Nibble 3	Nibble 2	Nibble 1
7th byte of response		6th byte of response		5th byte of response		4th byte of response	

4.1.6 *Keypad malfunction and service messages*

Upon detection of the appropriate event the unit will trigger Type 0 OTA update event or distress (transmission reason 91 (dec)) according to the programming bit on address 1710, bit 2 (event) and 1 (distress).

The message contains the STR as per the table below

STR	Description
0	Keypad Undefined Failure
1	Immobilizer device wires disconnection
2	Keypad locked
3	Relay malfunction
4	Ignition wire disconnected
5	Starter signal detection
6	Starter malfunction
7	Hotwiring Detection*
8	Primary cut unit failure
9	Secondary cut unit failure
10	Wrong keypad ID detected
11	Pairing Accomplished
12	Keypad flash failed
13	Alarm Cadence Activated by Keyb
14	Alarm Cadence Deactivated by Keyb
128	ECALL Initiated This message is generated 10 seconds before initiation of voice call as a real time message irrespectively to the setting in bits 1 and 2 of address

STR	Description
	1710 (dec)
129	BCALL Initiated This message is generated 10 seconds before initiation of voice call as a real time message irrespectively to the setting in bits 1 and 2 of address 1710 (dec)

* It is possible to auto-activate Alarm cadence upon detection of Hot Wiring, as per the programming bit on address 1710, bit 3.

4.2 Messages and Replies from AR system to Control Center

Replies to incoming commands are sent to the OTA channel as a content of Message type 9, sub data 0xB. The length of the expected ACK is provided in the command itself. The replies are described per command in the *Commands to Cello-AR Security Systems* section.

4.2.1 *OTA Messages Type 9, Sub-Data Type B from AR system*

Byte no.	Description	Containing
1	System code, byte 1	ASCII "M"
2	System code, byte 2	ASCII "C"
3	System code, byte 3	ASCII "G"
4	System code, byte 4	ASCII "P"
5	Message type	9
6	Unit's ID (total 32 bits)	Same as in Msg type 0
7		
8		
9		
10	Communication Control field	
11		
12	Message Numerator	
13	Packet Control Field	0x00
14	Total Data length	0d55
15	Sub-Data Type	B
16	Sub-Data Length	0d26
17	Length of actual data forwarded from 1-Wire channel	Length of Message code + Specific message code data

Byte no.	Description	Containing
18	Spare	
19-42	Message code + Specific message code data + Zero padding	Refer to *Commands to Cello-AR Security Systems* for the specific reply. The data length is normally shorter than 24 bytes; the extra bytes are zero padded.
43	Sub-data Type	4
44	Sub-data Length	0d25
45	Location status (flags)	See the following description of sub-data type 4 in Wireless protocol.
46	Mode 1 (from GPS)	
47	Mode 2 (from GPS)	
48	Number of satellites used (from GPS)	
49-52	Longitude	
53-56	Latitude	
57-59	Altitude	
60-61	Ground speed	
62-63	Speed direction (true course)	
64	UTC time – seconds	
65	UTC time – minutes	
66	UTC time – hours	
67	UTC date – day	
68	UTC date - month	
69	UTC date - year minus 2000 – 1 byte (e.g. value of 7 = year 2007)	
70	Check Sum	

4.2.2 *Response to a Keypad ID request*

Refer to the structure described in section keypad ID request.

Byte no.	Description	Containing
17	Length of actual data forwarded from 1-Wire channel	6

Byte no.	Description	Containing
18	Spare	0
19-42	Message code + Specific message code data + Zero padding	6 bytes of keypad ID + 18 bytes of zero padding

The first 3 bytes of the Keypad ID includes the Keypad Firmware version as follows:

byte[0] = Firmware sign character

byte[1] = Firmware High number

byte[2] = Firmware Low number

For example:

For Keypad ID: 50000A005050

byte[0] = Firmware sign character = '50' – 'P' in ASCII table

byte[1] = Firmware High number = 0

byte[2] = Firmware Low number = 0xA = 10

5 Commands to Cello-AR Security Systems

Every command to the AR system, except the (Read ROM) [33h], contains at least two bytes: the command code byte and command numerator byte. The content of the Command numerator is repeated in the reply for easy tracking of multiple commands. The command can also contain a data part. Read ROM command is an exception and contains only 1 byte: the command code [33h]

Long replies (longer than 3 bytes) are equipped with the CRC byte for a validity check from the receiving side.

5.1 Data Traffic from Control Center to AR system

Every information is communicated with the control center application as a payload of OTA Message type 9, sub data type 0xB. Incoming OTA Messages type 9, sub-type B are treated by the AR system only if AR keypad Support is enabled in programming, otherwise the command is ignored.

The system will generate an appropriate ACK to OTA Messages type 9 as defined per command.

Sub-Data B Module Structure

Byte Number	Byte Data	
N	Sub-data type	B
N+1	Sub-data length	Variable (Refer to table below) ***If this field is 0, the unit will respond with keypad ID***
N+2	Length of data to be forwarded to 1-Wire port	Actually (Sub-data length-2)
N+3	Length of expected reply from the keypad to be forwarded back from 1-Wire port	Refer to Cello AR 1-Wire Interface Protocol
N+4	Command Type	Refer to table below
N+5 – N+x	Command Data (optional, variable length, in some cases missing)	Refer to Cello AR 1-Wire Interface Protocol

Command Types table

Command name	Command Type	Data
Reset Keypad	[80H]	1 byte
Keypad ID Request (read rom)	[33H]	No Data

Feedback to Driver	[81H]	3 bytes
Set Operational State	[82H]	2 bytes
Time Update	[83H]	4 bytes
C&L Time/Date Settings	[84H]	4 bytes
Access Code Programming	[85H]	3 bytes
C&L Code Programming	[86H]	3 bytes
System Code (multicode) Programming	[87H]	3 bytes
Status Request	[89H]	1 byte
Code Request	[8AH]	2 bytes
C&L Times Batch Programming	[8BH]	7 bytes
Driver Code Control Command	[8CH]	4 bytes
Read C&L Time/Date Settings	[8DH]	1 byte
Miscellaneous Instructions	[8DH]	3 byte

5.2 Reset Keypad [80h]

This command allows the resetting of the keypad. The command contains 2 bytes: [Cid] 80

The system responds with 2 bytes: [Cid] 80 before a reset is actually performed.

Cid is a Command numerator, repeated by the system in a reply.

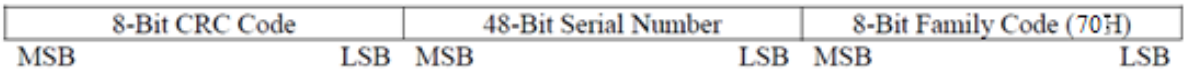
Command numerator	80h
2nd byte of response	1st byte of response

5.3 Keypad ID request (Read ROM) [33h]

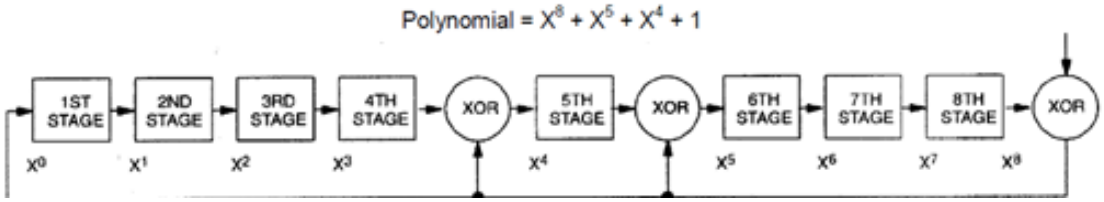
In order to query the Active keypad ID the Sub-data length field shall contain "zero". The command itself contains a single byte.

This command allows reading the keypad's 8-bit family code (70h), unique 48-bit serial number, and 8-bit CRC.

64-BIT LASERED ROM Figure 3



1-WIRE CRC GENERATOR Figure 4



5.4 Feedback to driver [81h]

This command allows operating the keypad's visual or audio signal to a driver.

After issuing the feedback to a driver command, the 2-bytes feedback definition is provided.

The command is in 2 bytes:

First byte of Feedback Definition	Second byte of Feedback Definition	Command numerator	81h
4th byte of command	3rd byte of command	2nd byte of command	1st byte of command

The system responds with responses of 2 bytes before the feedback is actually activated:

Command numerator	81h
2nd byte of response	1st byte of response

Feedback Definition

First byte							
Number of repetitions				Feedback source Buzzer LED1 LED2 LED3 4-15 – unused			
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Second byte							
Spare							Length of pulse 0 – short 1 - long
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

5.5 Set Operational State [82h]

This command allows setting the system operational state.

After issuing the Set Operational State command and its ID, the 1-byte Operational Set definition is provided.

The command is 3 bytes:

Operational Set definition byte	Command numerator	82h
3rd byte of command	2nd byte of command	1st byte of command

The system responds with responses of 2 bytes:

Repetition of the Command numerator	82h
2nd byte of response	1st byte of response

Operational Set definition							
Reserved					Desired Operational State		
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Desired Operational State Table

Number	State Name	State Description
0	Disarmed state	The immobilizer is not active and the vehicle can be used.
1	Standby state (infrastructure, currently not supported)	After ignition off the driver has the option to use the vehicle without authentication process for a programmable time period.
2	Armed state	The immobilizer is active and vehicle usage is dependent on the driver authentication process.
3	Keypad locked state	The immobilizer is active and the driver authentication process is restricted for a programmable time period. (For information only. Impossible to set this state by command)
4	Service / garage state	The immobilizer is not active and the vehicle can be used without authentication process due to suspicious user operation.
5-7	Reserved	

5.6 Time update [83h]

This command allows setting keypad's (security logic) current time.

After issuing the Time update command with its ID, the 3-bytes of time definition are provided.

First byte of Time Definition	Second byte of Time Definition	Third byte of Time Definition	Command numerator	83h
5th byte of command	4th byte of command	3rd byte of command	2nd byte of command	1st byte of command

The system responds with responses of 2 bytes.

Repetition of Command numerator	83h
2nd byte of response	1st byte of response

Time Definition

First byte							
Min (LSBits)		Seconds					
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Second byte							
Hours(LSBits)				Minutes (MSBits)			
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Third byte							
Validity bit Valid Invalid	Unused (Zeros)			Weekday (0 – Sunday, 1 – Monday etc)			Hours (MSBit)
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

5.7 C&L Time/Date Settings [84h]

This command allows programming working time for the specific weekday. The rest of the day will be considered C&L time.

The system will automatically enter C&L mode (requires C&L code instead of normal authorization code) in the non-working time (only if working time is set for at least one weekday).

After issuing the C&L Time/Date Settings command and its ID, the 3-bytes of time definition are provided.

The command contains 5 bytes:

The first byte of Working Time Definition	The second byte of Working Time Definition	Third byte of Working Time Definition	Command numerator	84h
5th byte of command	4th byte of command	3nd byte of command	2nd byte of command	1st byte of command

Time Definition

First byte							
Working Time Start Hours LSBits (in 24h format)			Working Time Start Minutes (15 minutes resolution)		Weekday (0 – Sunday, 1 – Monday etc)		
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Second byte							
Working Time End Hours LSBits (in 24h format)				Working Time End Minutes (LSBits) (15 minutes resolution		Working Time Start Hours MSBits (in 24h format)	
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Third byte							
Unused							Working Time End Hours MSBit (in 24h format)
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

The system responds with responses of 2 bytes.

Repetition of Command numerator	84h
2nd byte of response	1st byte of response

5.8 Access Code programming [85h]

This command allows programming of an access code, allowing the driver to de-immobilize the vehicle in work time.

After issuing the Access Code Programming command and its ID, the 2-bytes code definition is provided.

Char 3	Char 2	Char 1	Char 0
Byte 1		Byte 0	

For instance, for code 1234:

4	3	2	1
Byte 1		Byte 0	

The command contains 4 bytes:

Byte 0 of code (chars 0 and 1)	Byte 1 of code (chars 2 and 3)	Command numerator	85h
4th byte of command	3rd byte of command	2nd byte of command	1st byte of command

The system responds with responses of 2 bytes:

Repetition of Command numerator	85h
2nd byte of response	1st byte of response

5.9 C&L Code programming [86h]

This command allows programming of an access code, allowing the driver to de-immobilize the vehicle during C&L time.

After issuing the C&L Code programming command and its ID, the 2-bytes code definition are provided.

Char 3	Char 2	Char 1	Char 0
Byte 1		Byte 0	

The command contains 4 bytes:

Byte 0 of code (chars 0 and 1)	Byte 1 of code (chars 2 and 3)	Command numerator	86h
4th byte of command	3rd byte of command	2nd byte of command	1st byte of command

The system responds with responses of 2 bytes.

Repetition of Command numerator	86h
2nd byte of response	1st byte of response

5.10 System Code programming [87h]

This command allows the programming of the system code, allowing the calculation of the authorization code for the multi-code method. If this code is set to a value different from '0000', the system will automatically enter the multi-Code authentication method.

After issuing the system code programming command and its ID, 2-bytes code definition is provided.

Char 3	Char 2	Char 1	Char 0
Byte 1		Byte 0	

The command contains 4 bytes:

Byte 0 of code (chars 0 and 1)	Byte 1 of code (chars 2 and 3)	Command numerator	87h
4th byte of command	3rd byte of command	2nd byte of command	1st byte of command

The system responds with responses of 2 bytes:

Repetition of Command numerator	87h
2nd byte of response	1st byte of response

5.11 Keypad Status Request [89h]

This command allows requesting status of the keypad and the security system.

The command contains 2 bytes: [Cid] [89h]

The keypad responds with the following 14 bytes data frame:

CRC (8 bits)	Last Detected Code (32 bits)	Last Detected Code Recognition Status (8 bits)	Last detected Malfunction number (8 bits)	Operational state (8 bits)	Status bitmask (8 bits)	Current time (24 bits)	Repetition of Cid (8 bits)	89h (8 bits)

Current time

The current time structure can be found in Time update [83h] command

Status bitmask

Reserved for future usage		Immobilizer Status 0 – off 1- on	Ignition Status 0 – off 1- on	Access code set not set set	C&L Code set not set set	System Code Set not set set	Pairing Status (0) not paired (1) Paired
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Operational State Table

Number	State Name	State Description
0	Disarmed state	The immobilizer is not active and the vehicle can be used.
1	Standby state (infrastructure, currently not supported)	After ignition off the driver has the option to use the vehicle without authentication process for a programmable time period.
2	Armed state	The immobilizer is active and vehicle usage is dependent on the driver authentication process.
3	Keypad locked state	The immobilizer is active and the driver authentication process is restricted for a programmable time period. (For information only. It is not possible to set this state by command.)
4	Service / garage state	The immobilizer is not active and the vehicle can be used without authentication process due to suspicious user operation.
5-255	Reserved	

Malfunction / Alert number table

Number	Description
0	Keypad Undefined Failure
1	Immobilizer device wires disconnection
2	Keypad locked
3	Relay malfunction
4	Ignition wire disconnected
5	Starter signal detection
6	Starter malfunction
7	Hotwiring detection
8	Primary cut unit failure
9	Secondary cut unit failure
10-11	Reserved
12	Keypad flash failed
13-255	Reserved

Recognition Status

Reserved	Immobilizer Status 0 – off 1- on	Ignition Status 0 – off 1- on	Authentication (multi-code) Code status 2- OK 3- Wrong	Code status 2- OK 3- Wrong	Code type 4- Standard 5- Authentication 6- C&L 7- 7 - reserved		
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Last Detected Code

The code format is explained in Code Request [8Ah] command

5.12 Code Request [8Ah]

This command allows the requesting the codes programmed in the system.

After issuing the Code Request command with its ID, the 1 byte description is provided.

The command contains 3 bytes:

Code Request Description	Command numerator	8Ah
3rd byte of command	2nd byte of command	1st byte of command

Code Request Description:

0 – Access Code

1 – C&L Code

2 – System Code

3-255 - unsupported

The system responds with the following 8 bytes data frame:

CRC (8 bits)	The Code (32 bits)	Code description (8 bits)	Repetition of Command numerator	8Ah
Byte 8 of response	Bytes 4-7 of response	3rd byte of response	2nd byte of response	1st byte of response

The Code (32 bits)

Master code, only in case of reply to access code request, otherwise sent as zeros				LSB char of the code	3rd char of the code	2nd char of the code	MSB char of the code
LSB char of Master code	3rd char of the Master code	2nd char of the Master code	MSB char of Master code				
Nibble 8	Nibble 7	Nibble 6	Nibble 5	Nibble 4	Nibble 3	Nibble 2	Nibble 1
7th byte of response		6th byte of response		5th byte of response		4th byte of response	

Example of response for user code is 1122 and master code is 2211, command numerator 0.

0x8A 0x00 0x11 0x22 0x22 0x11 0x(crc)

5.13 C&L Times batch programming [8Bh]

This command adds the batch programming option to the command 86h described above, and allows programming working time for all days in the week in one command.

The command provides an infrastructure for programming the entire working week by a single command; it provides 2 templates of working time.

Each template provides a bitmask for the weekday's selection and for the hour of work start and work end. No minute resolution is supported by this command; the system automatically enters minutes as 00 when preceding this command.

The system automatically enters C&L mode (requires the C&L code instead of normal authorization code) during the non-working time (only if the working time is set for at least one weekday).

After issuing the C&L Times batch programming command with its ID, the 6 bytes of configuration are provided as follows:

Weekdays	Start hour	End hour	Weekdays	Start hour	End hour	Command numerator	8Bh
Template 1			Template 2				
8th byte of command	7th byte of command	6nd byte of command	5th byte of command	4th byte of command	3nd byte of command	2nd byte of command	1st byte of command

Weekdays

0	Sat	Fri	Thu	Wed	Tue	Mon	Sun
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

The system responds with the following data frame:

Repetition of Command numerator	8Bh
2nd byte of response	1st byte of response

5.14 Driver's Code Control [8Ch]

This command provides an infrastructure for enabling and disabling certain driver codes for usage in Multi-Code mode. Since there are only buttons from 1 to 5 there are 625 code options from 1111 to 5555. Each such code is equipped with an index from 1 to 625, as follows:

Code	Index
1111	1
1112	2
1113	3
…	…

Code	Index
5553	623
5554	624
5555	625

The following relation exists between the index and the code:

When the code is 4 chars as follows: $X^1X^2X^3X^4$ (In case of Code 4321 the $X^1 = 4, X^2 = 3, X^3 = 2$ and $X^1 = 1$)

Index = (X^4-1) + (X^3-1)*5 + (X^2-1) * 25 + (X^1-1) * 125 + 1

The command provides a capability to enable or disable up to four driver codes at once, as well as clearance of the entire list of blocked codes.

10 bits of Index to Code D MSB	10 bits of Index to Code C	10 bits of Index to Code B	10 bits of Index to Code A LSB	Control Byte	Command numerator	8Ch
8th byte of command	7th byte of command	6nd byte of command	5th byte of command	4th byte of command	3nd byte of command	2nd byte of command	1st byte of command

Control byte

Spare			Erase Blocked Codes List 0 – Do not erase 1- Erase	Block Code of Index D 0- Enable 1 - Block	Block Code of Index C 0- Enable 1 - Block	Block Code of Index B 0- Enable 1 - Block	Block Code of Index A 0- Enable 1 - Block
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

The system responds with the following data frame.

Number of Blocked Codes in keypad's memory (before the performance of the command) LSB		Repetition of Command numerator	8Ch
4th byte of response	3rd byte of response	2nd byte of response	1st byte of response

5.15 Reading C&L Setting [8Dh]

The command allows the reading of C&L settings from the configuration memory of the unit.

Command numerator	8Dh
2nd byte of command	1st byte of command

The system responds with the following data 12 bytes frame:

MSB	8Ch							
2nd byte	Repetition Command numerator							
3rd byte	Sunday							
	End Time (LSB)			Start rime				
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
4th byte	Monday						Sunday	
	End Time (LSB)	Start rime					End Time (MSB)	
	Bit 0	Bit 0	Bit 0	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
5th byte	Tuesday				Monday			
	Start rime (LSB)				End Time (MSB)			
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
6th byte	Wednesday		Tuesday					
	Start rime (LSB)		End Time (MSB)					Start rime (MSB)
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
7th byte	Wednesday							
	End Time					Start rime (MSB)		
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
8th byte	Thursday							
	End Time (LSB)			Start rime				
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
9th byte	Friday						Thursday	
	End Time (LSB)	Start rime					End Time (MSB)	
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
10th byte	Saturday				Friday			
	Start rime (LSB)				End Time (LSB)			
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
11th byte	SPARE (zeros)		Saturday					
			End Time					Start rime (MSB)
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
12th byte	CRC							

5.16 Miscellaneous instructions [8Eh]

This command enables the activation of different functions by using 3 data bytes structure.

After issuing the function control command with its ID, the 3 bytes of data are provided:

Data for features activation			Command numerator	8Eh
3th byte	2nd byte	1nd byte	2nd byte of command	1st byte of command

The system responds with the following data frame:

Repetition of Command numerator	8Eh
2nd byte of response	1st byte of response

The supported features are as follows:

3th byte	2nd byte	1st byte	Description
0	0	FF	Disable hotwiring detection
0	1	FF	Enable hotwiring detection
0	0	FE	Disable entering code when ignition is on
0	1	FE	Enable entering code when ignition is on
0	The time in resolution of 30 seconds (4 for 2 minutes, 10 for 5 minutes)	FD	Set up time for immobilizer arming (after ignition off)