Cello-AR Security

Product Overview

Cellocator Division
Pointer Telocation Ltd.

Proprietary and Confidential

Version 1.1

Revised and Updated: January 20, 2013

POINTER

Table of Contents

1 Introduction

1.1 Purpose and Scope

This document summarizes the relevant information regarding the additional features and capabilities of the Cello-AR Security system, compared with the Cello-F.

The document is intended for Fleet Management or SVR service providers, system integrators, fleet managers or technical personnel who want to understand the capabilities and functionality of the system. Integration information is provided in the *Cello-AR Integration Manual*.

The document describes the system functionality, architecture, features, driver and technician operating instructions, installation procedures, evaluation steps, and technical specifications.

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.

1.2 References

#	Reference	Description
1	Cello-AR introduction	
2	Cello-AR Integration Manual	

1.3 Definitions, Acronyms, Abbreviations

Abbreviation	Description
ECall	Emergency Call
BCall	Breakdown Call
OTA	Over The Air
FOTA	Firmware update Over The Air
C&L	Clock and Lock
GPRS	General Packet Radio Service

1.4 Revision History

Version	Date	Description
1.0	13/09/2011	First draft
1.1	20/01/2013	Approved document

2 Product Description

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.
- A robust and smart immobilizing system with a redundancy option.
- Theft or tamper attempt 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 by the control center application.

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.
- Pairing between the AR-Keypad and the smart immobilizers, and between the Cello-AR unit and the AR-keypad. 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.
- Towing detection.
- Jamming detection and reaction.

The Cello-AR Security system consists of a keypad, immobilizers and the Cello-AR unit. The smart immobilizers utilize relay for deactivating the vehicle engine and maintaining wire or wireless communication with the AR-Keypad. The AR-Keypad, via which the driver/technician interacts with the system, controls the immobilizers. The 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.

2.2 Main Functionality

The new Cello-AR Security product was designed to provide a cost-effective solution with enhanced anti-theft features and functionality.

Complete with a user-friendly keypad interface via which the driver can intuitively interact with the system, this new anti-theft security system provides the following main functionality:

- Allows vehicle usage only to authorized and identified drivers.
- Detects theft or tamper attempts and reports these attempts to the control center (early alert).
- Allows online monitoring of the vehicle status and driver activities.
- Allows online control of the vehicle security state and user assistance, where users can call the customer center and receive support/service via OTA commands (including a new password, or disarming the car if the user forgets their password or the keypad malfunctions).

2.3 Main Features

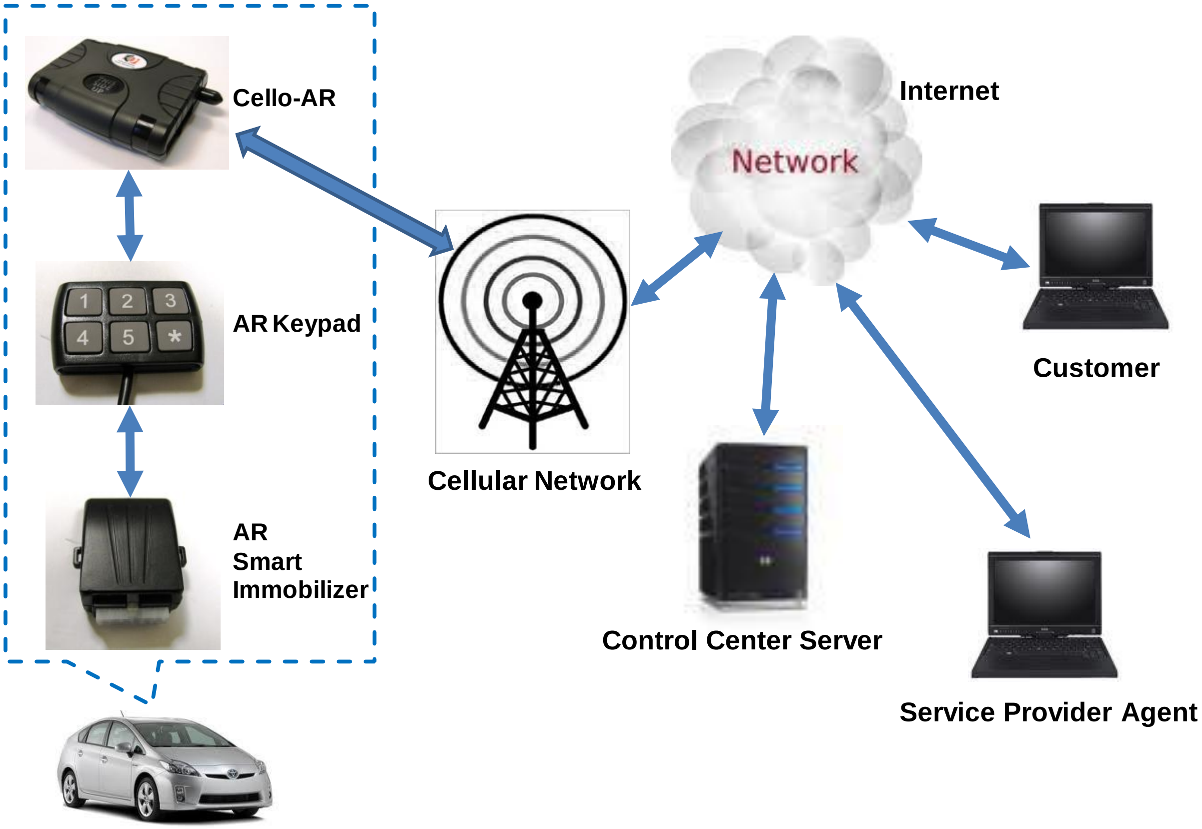
This section gives an overview of the main features that provide the functionality described in the previous section. A more detailed description of these features can be found in the *Cello-AR Security* System Features section.

- Secured vehicle usage by authorized and identified drivers is ensured via three methods:
    - Unique **user codes.**
    - Unique **authentication code** in addition to the **user code (Multi-Code**).
    - An emergency disarming option using the ignition switch.

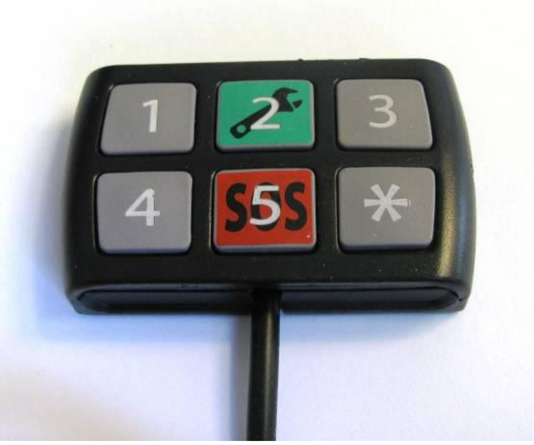
  Further security is provided with the Clock and Lock feature which restricts vehicle usage to specific times, even to authorized drivers.
- Theft and tampering attempts are prevented by the communication and pairing process between the **smart immobilizer(s)** and the **AR Keypad**, in addition to the communication and pairing process between the AR-Keypad and the Cello-AR, which ensures any disconnection or removal of any AR component invokes an alarm. In addition, **secured OTA and serial communication** with the control center prevents the replacing of the Cello-AR unit.
- Drivers can **ECall** and **BCall** using Cellocator Hands Free.
- Online **monitoring of the vehicle security system via OTA, including security states, driver activity** and **theft / tampering attempts** ensures immediate involvement of control center personnel when needed, as well as immediate assistance for the driver on any problematic state, even before the driver calls the control center.
- Online **user assistance** is performed via **OTA communication with the control center**, which enables the control center personnel to assist the driver remotely without the need to physically be there at the vehicle. For example: vehicle access can be granted by changing the vehicle security state from armed to unarmed, the user code changed, and system programming parameters modified. See also the *Technician Operating Instructions* section.

2.4 System Architecture and Components

The main components of the Cello-AR Security system include the Cello-AR, a keypad and wired and smart immobilizer. This section describes these main components, as shown in the following diagram.



2.4.1 *AR Keypad*



The AR keypad is the interface of the system. It is used to control the system and manage system states, including driver authentication, password changes, Ecall, BCall and any operation which requires driver or technician inputs.

The keypad features six push buttons and six LEDs. The keypad enables the user to enter a user code, to program the Cello-AR system and provides LED and buzzer indication on various system states. The keypad supports Ecall via the red button and Bcall via the green button.

The keypad has wired and wireless interfaces for communicating with the AR smart immobilizer and Cello-AR system. The keypad also requests a time update from the Cello-AR unit every six hours.

The keypad has two kinds of one wire interface communications: **SNet** for communication with the smart immobilizers and **1-wire proprietary protocol** for communication with the Cello-AR.

2.4.2 *AR Smart Immobilizer*

This is an independent unit that performs physical disconnection of the vehicle circuit by means of an electrical relay. The Cello-AR Security system provides two kinds of smart immobilizer; wire and wireless. All smart immobilizers are managed through the keypad via SNet communication. The wired AR Immobilizer is provided with a dedicated harness including status led.

2.4.3 *Cello-AR*

The Cello-AR is a special variant of the Cello Family which supports the special features and capabilities required by the Cello-AR Security system.

The Cello-AR utilizes special Firmware for supporting the advanced security features required by the system, in addition to the regular features of the Cello-F. The 1-wire interface is used for communication with the AR keypad and consequently all Dallas based devices (Dallas key reader, Cellocator keypad and Cellocator proximity reader) cannot be connected to the Cello-AR and the Driver ID feature is not functioning.

The Cello-AR unit as a security system, which required detecting immediately any security event, is not designed for operation in full hibernation mode. Also, in full hibernation mode, the communication with the AR-keypad is not operable and might be considered as tamper attempt by the AR Keypad.

2.4.4 *SNet protocol*

SNet is a proprietary, one wire, serial protocol that provides a standard interface between the AR keypad and wired smart immobilizer. The SNet employs a master slave scheme; the keypad is a master node on the bus, and smart immobilizers are slaves.

2.4.5 *1-wire protocol*

A proprietary protocol based on a 1-wire interface provides a communication channel between the Cello-AR and the AR-Keypad.

2.5 System Operation Basics

This section describes the basic operations performed by the Cello-AR Security system, including how inputs are received and processed, and the outputs generated. It also includes an overview of how the system typically works.

2.5.1 *System inputs*

There are a number of inputs to the Cello-AR Security system:

- Diagnostic events that indicate theft or tampering attempts are detected by sensing the electronic signals generated by the vehicle.
- Driver and technician inputs are received via the AR keypad.
- Control center commands, received via OTA.

2.5.2 *Operations performed*

A number of operations are performed by the Cello-AR Security system:

- Interaction is maintained with the driver and/or technician via the AR keypad, namely through audio and visual indications (LED and buzzer).
- Vehicle usage is permitted or prevented, and security states managed, according to the inputs received.
- Communication disturbances, invalid or incorrect keypad usage, improper vehicle electronic signal and pairing violations that are detected are considered tamper or theft attempts; vehicle usage may be denied and relevant communication forwarded to the control center.
- Commands received OTA from the control center are performed as required.

- Ecall and Bcall voice calls to emergency or service centers. The driver activates these features via the AR keypad.

2.5.3 *Outputs generated*

A number of outputs are generated by the Cello-AR Security system:

- Vehicle usage can be disabled via the AR smart immobilizer.
- Monitoring reports on the vehicle status and user / technician activities are sent to the control center, either periodically or immediately on the occurrence of specific events (such as when the user code is entered).
- Indications (both visual and audio via LED and buzzer) are generated for the benefit of the driver / technician from the AR keypad.

2.5.4 *Normal Operation Procedure*

In order to use the vehicle, the driver enters their secret password using the keypad. As a result the immobilizer is deactivated, allowing vehicle usage and the system enters the disarm state.

When the driver terminates the usage of the vehicle by switching off the engine, the system enters standby state for the preprogrammed time period, allowing the driver to reuse the vehicle without entering the password.

When the timeout of the standby state elapses, the system is activated and the system enters the arm state, disabling the usage of the vehicle and issuing alerts upon detection of theft attempts.

3 Cello-AR Security System Features

This section describes the various Cello-AR Security system and configuration features and options, including the following:

- **Security Operational States**
- **System Anti-Theft Protection**
- **Driver Identification and Authentication**
- **Pairing of the AR Components (Cello-AR, AR Keypad and AR Immobilizer)**
- **Ecall and Bcall**
- **Diagnostic Events Detection and Reporting**
- **System Reports to the Control Center**
- **Commands Received from the Control Center**
- **Additional Special Features**

3.1 Security Operational States

The Cello-AR Security system provides the following states:

- **Disarmed:** This is the non-secured mode of the system. The immobilizer is not active and the vehicle can be used.
- **Standby:** After ignition is switched off, the driver has the option to use the vehicle without performing the authentication process for a programmable time period.
- **Armed:** This is the secured mode of the system. The immobilizer is active and the vehicle cannot be used. Vehicle usage is dependent on the driver authentication process.
- **Keypad locked:** This is a high secured state initiated automatically by the system when a possible theft attempt is detected. After an invalid user code has been entered four times, the system blocks keypad usage and remains in this state for a predefined period of time. The immobilizer is active and the vehicle cannot be used.
- **Service / garage:** This is a non-secured mode in which the system allows free access to the vehicle and will not automatically switch to armed state. The immobilizer is not active and the vehicle **can** be used without the authentication process. This feature is especially useful when the vehicle is being repaired, allowing free access to the vehicle by repair personnel.
- **Clock and lock:** This is a high secured state preventing vehicle access for certain programmable time periods per day, even for authorized drivers. The immobilizer is active and the vehicle cannot be used. In addition, the driver authentication process is restricted according to the Clock and Lock programmable time period (for one day in the week); vehicle usage is restricted even if a regular valid code is entered.

The system provides a visual device (LED) with different visual indications for each state.

Note that the changing of states, as described in the following sections, can be performed via OTA commands.

3.1.1 *Disarming the system*

In the Disarmed state the system enables the vehicle engine to be switched on or the vehicle be driven. The system can be disarmed via several methods:

- **Disarming through the keypad:** The driver can disarm the system using the keypad in several ways, as described in the *Driver Identification and Authentication* section. The operating instructions are described in the *Driver Operating Instructions* section.
- **Disarming through OTA command:** The security system will switch to the Disarmed state on receiving a disarm command from the control center application.
- **Disarming through the ignition switch (emergency disarm):** This method is used when keypad usage is impossible due to keypad malfunctions or other reasons, and the driver cannot communicate with the control center or GPRS communication is not available. The driver is able to disarm the system with the help of the vehicle ignition switch, as described in the *Driver Operating Instructions* section.

  Note that the system will initiate an alert (through audible and visual signals) if one of the immobilizers fails to be deactivated, or an immobilizer has not completed the pairing synchronization process.

3.1.2 *Arming the system*

Arming the system means physically activating the immobilizer(s). In this case, the system will prevent the ignition of the vehicle's engine. The Armed state can be employed only when the ignition is turned *off.* The system can be armed via several methods:

- **Arming via the keypad:** The driver can arm the system using the keypad. The operating instructions are described in the *Driver Operating Instructions* section.
- **Automatically (Passive arming):** After 120 seconds in the Disarmed state and ignition switched off, the system will perform an automatic arm procedure (passive arming). This is done to ensure the car is secure even though the driver failed to arm the system. Note that passive arming is disabled while Service state is active.
- **Arming through OTA command:** The security system will switch to Armed state on receiving an arm command from the control center application.

  On entering the Armed state the keypad plays an arm sound alert and the * red LED will blink according to the Armed state pattern.

  The system automatically activates the pairing process between the AR Keypad and the immobilizers, saving the need for manual pairing activation.

3.1.3 *Entering and exiting Service state*

Entering Service state

It is possible to enter the Service state through one of the following methods:

- **Via keypad:** The driver can switch the system to Service state by using the keypad. The operating instructions are described in the *Driver Operating Instructions* section.
- **Via OTA command:** The security system will switch to Service state on receiving the relevant command from the control center application.

Exiting Service state

The system can be switched from Service state to Armed or Disarmed state in one of the methods described above.

3.1.4 Entering and exiting Keypad Locked state

Entering Keypad Locked state

The system automatically enters Keypad Locked state from the Armed state only, after four attempts of entering an illegal user code.

Exiting Keypad Locked state

The system can switch to Armed or Disarmed state through one of the following methods:

- Exit to Armed state automatically when the pre-programmed time period has elapsed.
- Switch to Disarmed state via the keypad by entering the master code.
- Exit to Disarmed or Armed state via OTA command.
- Switch to Disarmed state via the emergency disarming process.

3.1.5 Entering and exiting Clock & Lock state

Entering Clock & Lock state

The system switches to Clock & Lock state automatically according to a programmable time slot per day in the week.

Exiting from Clock & Lock state

The system can be switched to Armed or Disarmed state through one of the following methods:

- Switched to Armed state by entering a special password for the Clock & Lock state, provided by the fleet manager. The driver should then disarm the system in one of the methods described above.
- Switched to Armed state automatically when the pre-programmed time period has elapsed.
- Switched to Disarmed or Armed state via OTA command.

3.2 System Anti-Theft Protection

The Cello-AR Security system ensures anti-theft protection via the detection of the following events:

- **Disconnection of communication between the keypad and the Cello-AR:** If the system identifies a communication malfunction for 30 continuous seconds it will send a communication error alert message to the control center application, and play a short beep and blink every second.
- **Disconnection of communication between one of the smart immobilizers and the keypad:** The keypad manages a keep alive process to verify the correct immobilizer state, and to identify communication malfunctions. After 60 continuous seconds of communication malfunction the keypad sends a communication error alert to the control center application. The immobilizer activates its relay (disables the vehicle engine) on lack of communication for more than five continuous minutes (immobilizer passive arm).

- **Engine activation in Armed state (Hot wiring):** The system detects engine activation in the system Armed state and reports the event to the control center application.
- **Towing detection:** The system detects vehicle towing and reports it to the control center application.
- **Jamming detection and reaction:** The system detects jamming attempts and reports to the control center application. In addition, the system activates pre-programmed output for programmed cadence.
- **Replacement of the keypad or immobilizer:** Replacement of the keypad or immobilizer is detected via a pairing violation. AR components will not communicate with the other paired device if the expected pairing is violated. Consequently, the immobilizer(s) enters a passive armed state and disables vehicle usage. The system reports on the pairing violation detection to the control center application.
- A **Security Alarm** is the activation of selected Cello-AR outputs for a session of sequential pulses, used for visual and audio alarm notification. Security Alarm can be activated by an OTA command, or by internal logic further to the detection of a wrong keypad ID or keypad disconnection.

3.3 Driver Identification and Authentication

The Cello-AR Security system supports two methods of driver identification and authentication according to programmed parameters:

- The basic method uses a **user code** of four digits. The system compares the user code which is entered by the user via the keypad with a preprogrammed user code, and disarms the system if they are found to be equal.

  The system is shipped with a unique user code generated during manufacturing from the keypad serial number. The original user code can be always derived from the keypad serial number, if provided. The user code can be subject to change at anytime via OTA command or by the user via the keypad. Note that after the first time the user code is changed it will be impossible to decode the user code from the keypad serial number.
- The **multi code** is a highly secure and sophisticated authentication method which uses a four digit authentication code *in addition* to the basic four digit user code (described above).

  Unlike the basic method, the system manages a black list (unauthorized) of user codes which are programmed into the system. However, as with the user code, the authentication code is provided by the manufacturer.

  The authentication code is generated by a special algorithm using the user code and system code as inputs. The system code is a four digit number defined by the fleet manager and is normally used for the whole fleet. The system number is programmed into the system.

  For authentication, the user has to enter the user code and then the authentication code. The system compares the entered user code with the programmed black list, then the system generates the authentication code from the entered user code and the programmed system codes and compares it with the entered authentication code. The system switches to Disarmed state only if the user code and authentication code are valid. The authentication code is immune to hackers as it is not programmed in the system and not transferred OTA, and therefore the security level of the system is much stronger.

The **master code** is a four digit number used (by a technician) to unlock a system which is in Keypad Locked state. The master code is shipped with the keypad.

3.4 Pairing the AR-Keypad and AR-Immobilizer

The system maintains pairing between each immobilizer and the keypad, and between the keypad and the Cello-AR unit. Pairing synchronization is activated on installation, either by a technician using the keypad or via OTA Arm command. Once pairing is synchronized, an AR component will not communicate with the other paired device if the expected pairing is violated. Consequently, the immobilizer(s) enters a passive armed state and disables vehicle usage. The system reports on the detection of a pairing violation to the control center application.

Each AR smart immobilizer is provided with a unique pairing code of four digits. The pairing code is derived from the immobilizer serial number. The pairing code of each immobilizer is entered into the system by the technician using the keypad, which in turn enables pairing synchronization.

The system also supports automatic pairing synchronization via an OTA Arm command, which prevents the technician from having to program pairing codes.

3.5 Pairing the AR-Keypad and the Cello-AR

The Cello-AR unit and the AR-keypad continually maintain pairing checks, if programmed accordingly. The pairing synchronization is activated by the technician on installation.

If programmed accordingly, and an invalid (not paired) keypad is detected, the Cello-AR activates a preprogrammed alarm indication of preprogrammed cadence, and reports to the control center application.

The AR-keypad indicates a pairing violation by activating the buzzer in the fail cadence.

3.6 Ecall and Bcall

The system supports a convenient way of initiating emergency calls to an emergency center and breakdown calls to a service center. The destination telephone numbers are preprogrammed via OTA. The driver activates these features via the keypad. Note that these features are available only if the Cellocator Handsfree module is installed.

3.7 Additional Special Features

The Cello-AR Security system supports up to five special features which can be activated by the user by pressing *, followed by one of the digits 1-5. These five special features are defined by the backend application; the Cello-AR system simply informs the backend application that the user has activated feature *1, *2, *3, *4 or *5.

The activation of these features is reported to the control center application, which performs the relevant operations and activities as defined by the service provider.

The feature can be activated only in disarmed state.

3.8 System reports sent to the control center.

This section describes the various reports that are sent to the control center application.

The Cello-AR Security system reports (by sending messages) on the following events:

- User enters an access code using the AR keypad
- User activates a special feature
- Malfunction and service events are detected:
  - Communication disconnected between the keypad and the immobilizer for at least 60 seconds
  - Relay malfunction
  - Security state change
  - Ignition wire disconnected
  - Starter signal detection
  - Starter malfunction
  - Hotwiring Detection - the vehicle engine is switched on while in Armed state
  - Primary/secondary immobilizer failure
  - AR-Keypad pairing violation
  - AR-Keypad pairing synchronization accomplished
  - Keypad flash failed
  - Security alarm activated by keyb
  - Security alarm deactivated by Keyb
  - ECALL initiated
  - BCALL initiated

In addition to the event reporting, the system also reports continously on the current security state, the last received code, the communication status with keypad, and more in message 0.

Detailed information regarding the information provided by the system is described in the *Cello-AR Integration Manual*.

3.9 Commands Received from the Control Center

The following commands are received by the Cello-AR unit from the control center:

- Reset keypad and security state.
- Keyboard ID request.
- Activate feedback to driver:allows the operating of the keypad's visual (LEDs) or audio (buzzer) signals to a driver.
- Set security operational state.
- Update security logic time.
- Program Clock & Lock time/date: this command allows the programming of a working time for the one specific weekday. The rest of the day will be considered Clock & Lock time.

- Program access code: this command allows the programming of the four digit user code, granting vehicle usage to the driver.
- Program Clock & Lock bypass code: this command allows the programming of the four digit code allowing vehicle usage during Clock & Lock time.
- Program system code: this command allows the programming of the four digit system code, allowing the calculation of the authorization code for the multi-code method. If this code is set to a value other than '0000', the system will automatically enter the multi-code authentication method.
- Status request: this command allows the requesting of the status of the keypad and the security system.
- Code request: this command allows the requesting of the various codes programmed in the system (user code and master code, Clock & Lock, system code).
- Program Clock & Lock times batch: this command allows the programming of a working time for all days in the week in one command. The rest of the day will be considered Clock & Lock time.
- Program driver code control: this command allows the enabling and disabling of up to four driver codes for usage in the multi-code method, and the capability to block all possible codes.
- Clock & Lock time/date settings request: this command allows the reading of programmed Clock & Lock settings.

For further details on each of the above commands, refer to the *Cello-AR Integration Manual*.

3.10 System Indications

The system utilizes the keypad LEDs (5 blue on digits 1-5 and one red on the *) and the keypad buzzer system status and user feedback indications as described in the following sections.

3.10.1 *Keypad red LED indications*

State description	Red led indication
Arm state	250msec symmetric toggling **1 sec symmetric toggling in Sleep mode**
Disarm state with ignition off	LED on
Disarm state with ignition on	LED off
Keypad Locked state	4 blinks in 2 seconds
Service / garage state	2 blinks in 1 second and off 1 second
Primary immobilizer fails to deactivate the engine	LED1: 20 blinks of 500msec
Secondary immobilizer fails to deactivate the engine	LED2: 20 blinks of 500msec

State description	Red led indication
Programming session activated	Fast blinking 100msec symmetric toggling

3.10.2 *Illuminating blue LEDs (1-5)*

The illumination light comes on when pressing any keypad digit and lasts for a period of six seconds helping keypad activation in night.

3.10.3 *Keypad buzzer indications*

State/Action	Buzzer Sound
Short press of a button. Command received. Entering active armed command (*3333) during active armed activation.	Short beep
Legal disarm code entered. Pairing synchronization between keypad and immobilizer process successful. Emergency disarm successfully completed. Changing user code success. Pairing synchronization of keypad with Cello-AR successful.	Success sound
First new user code, during user code change process, is entered. User code, during multi-code disarming session, is entered.	Confirm sound
Illegal disarm code is entered. Pairing synchronization process failed. Emergency disarm failed. Changing user code failed.	Wrong sound
Entering Keypad Locked state. Ignition opened in Armed state.	Block sound (5 sec period)
Entering Armed state. Exit from program mode.	Long beep
Primary immobilizer is not paired. Secondary immobilizer is not paired.	Long beep and short beep

4 Driver Operating Instructions

This section describes the Cello-AR Security features that can be performed by the driver:

- **Disarming the System**
- **Disarming the System in Clock & Lock state**
- **Active Arming**
- **Passive Arming**
- **Changing the User Code**
- **Making an Emergency call (ECall)**
- **Making a Breakdown call (BCall)**
- **Activating a Special Feature**
- **Working in Service state**

4.1 Disarming the System

- **To disarm using the user code method:**
  - Press the * (star) button, followed by the four digits of the user code.
  - The keypad plays the disarm sound, and the keypad red LED indicates the Disarmed state. The vehicle is now ready for use.
  - If an unpaired immobilizer is detected, the keypad plays a long beep followed by a short beep three seconds after the disarm sound.
  - If one of the immobilizer units fails to deactivate the engine, the keypad plays the wrong sound and blinks 20 times.
  - On disarming failure, the keypad plays the wrong sound.
- **To disarm using the multi-code method:**
  - Press the * (star) button, followed by the four digits of the user code.
  - The keypad plays the confirmation tone.
  - Press the * (star) button followed by the four digits of the authentication code.
  - The keypad response is described in the previous section.
- **To disarm using the emergency method:**
  - Turn the ignition switch on and off according to your user code digits. One digit is equal to one on and off cycle of the ignition switch.
  - Wait five seconds before the next digit.
  - Wait five seconds with ignition off, after entering the last digit.
  - The keypad response is described above.
  - In case of failure, hold the switch in the off state for at least ten seconds to initiate a new session.

Example: To perform an emergency disarm with the user code 2342

1. First digit '2': switch the ignition on and off twice.
2. Wait five seconds.

3. Second digit '3': switch the ignition on and off three times.
4. Wait five seconds.
5. Third digit '4': switch the ignition on and off four times.
6. Wait five seconds.
7. Last digit '2': switch the ignition on and off twice.
8. Wait five seconds.
9. Turn on the ignition.
10. After five seconds the system is disarmed.

4.2 Disarming the system in Clock and Lock state

- **To disarm the system in Clock & Lock state:**
  - Call the fleet manager and get the special code for the Clock & Lock state.
  - Press the * (star) button followed by the four digits of the Clock & Lock code provided by the fleet manager.
  - The keypad plays the confirmation sound.
  - Continue with the regular method for disarming the system.

4.3 Active Arming

- **To arm the system:**
  - Press the * (star) button, followed by 3333.
  - The keypad plays a short beep for confirmation.
  - Press the * (star) button, followed by the four digits of the user code.
  - The keypad plays the arm sound and the red LED will blink according to arm state indication.
  - The system enters the Armed state.

4.4 Passive Arming

After 120 seconds in the Disarmed state and with ignition off, the system performs an automatic arming procedure (passive arming).

- The keypad plays the arm sound and the red LED will blink according to arm state indication.
- The system enters the Armed state.

4.5 Changing the User Code

You can change the user code to a new valid code. Note that the following codes are invalid: 1111, 2222, 3333, 4444, 5555, 1234 and 4321.

- **To change the user code:**
  - Disarm the system.
  - Switch on the ignition within the 30 second time window after disarming.

- Enter a new user code.
- The keypad plays one short beep for confirmation.
- Enter the new code again for verification.
- The keypad plays the success tone.
- On failure, or the entering of an illegal code, the keypad plays the wrong sound.

4.6 Making an Emergency call (ECall)

- **To call an emergency center:**

- Press the '5' digit for more than two seconds.
- The keypad plays three short beeps.
- Wait till the call is established. This could take several seconds or even longer if the cellular network experiences issues.

4.7 Making a Breakdown call (BCall)

- **To call service center:**

- Press the '2' digit for more than two seconds.
- The keypad plays three short beeps.
- Wait till the call is established. This could take several seconds or even longer if the cellular network experiences issues.

4.8 Activating a special feature

- **To activate one of the five special features:**

- Make sure that the system is in the Disarm state, or disarm the system.
- Press the * button for two or more seconds.
- Within five seconds press the appropriate digit (1, 2, 3, 4 or 5).
- The keypad plays two short beeps for confirmation.
- The keypad plays a success sound when a confirmation from the control center application is received.

4.9 Working in Service state

- **To activate the Service state:**

- Validate that the system is in Disarmed state, or disarm the system.
- Switch on ignition within 30 seconds.
- Press a long press on the '2' button (in this case, the long press on the '2' button will not activate a Bcall).
- The keypad plays the confirmation tone and the red LED blinks with Service state indication.
- The system is now in Service state and you can use the vehicle without performing the disarming process.

- **To exit the Service state:**

- Activate the active arm procedure to set the system to Armed state.
- Activate the disarming procedure to set the system into Disarmed state.
- Switch the ignition on for 20 minutes to set the system into Disarmed state. The keypad plays and the keypad red LED blinks with the Disarmed state indication.

5 Technician Operating Instructions

Technicians can activate all driver activities which do not require the unique codes of the driver. This section describes the features that can be performed by technicians only:

- **Disarming the System in Keypad Locked state**
- **Activate pairing synchronization**
- **Programming the System**

5.1 Disarming the System in Keypad Locked state

- **To disarm the system using the master code:**
  - Get the unique master code of the vehicle from the fleet manager and the unique user code from the driver.
  - Press the * (star) button, followed by the four digits of the master code.
  - The keypad plays the confirmation tone.
  - Within 10 seconds, press the * (star) button followed by the four digits of the user code.
  - The keypad response is described in the appropriate section of the driver operating instructions.

5.2 Programming the System

5.2.1 *Entering Programming mode*

The programming mode enables the technician to program and change some of the immobilizer system parameters.

- **To enter programming mode:**
  - Disarm the system. If the system is already in the Disarmed state you have to activate another state and then disarm the system.
  - Within 30 seconds, switch on the ignition.
  - Press a long press on the ‘3’ button.
  - The keypad plays the confirmation tone, and the keypad red LED blinks fast.

5.2.2 *Exiting Programming mode*

- **To exit programming mode:**
  - Switch off the ignition.
  - The keypad plays one long beep.

The system exits the programming session automatically after 30 continuous seconds without any keypad buttons being pressed.

5.2.3 *Activating pairing synchronization between the keypad and the immobilizers*

Pairing synchronization should be activated as part of the installation process.

- **To activate pairing synchronization process:**
  - Enter programming mode.
  - To pair the primary immobilizer: Press * followed by 1 and the four digits of the unique pairing code provided with the immobilizer.
  - To pair the secondary immobilizer: Press * followed by 2 and the four digits of the unique pairing code provided with the immobilizer.
  - To pair the wireless immobilizer: Press * followed by 3 and the four digits of the unique pairing code provided with the immobilizer.
  - The keypad plays the confirmation tone.
  - If the pairing synchronization fails, the keypad plays the wrong sound.

5.2.4 *Activating pairing synchronization between the keypad and the Cello-AR*

- **To activate the pairing synchronization process:**
  - Enter programming mode.
  - Press 51124.
  - The keypad plays the confirmation tone.
  - If the pairing synchronization fails, the keypad plays the wrong sound.

5.2.5 *Setting Programming parameters*

The technician can program various parameters which affect the operation of the system. The following table lists the various parameters and for each one the activation code and the audible confirmation indication are listed.

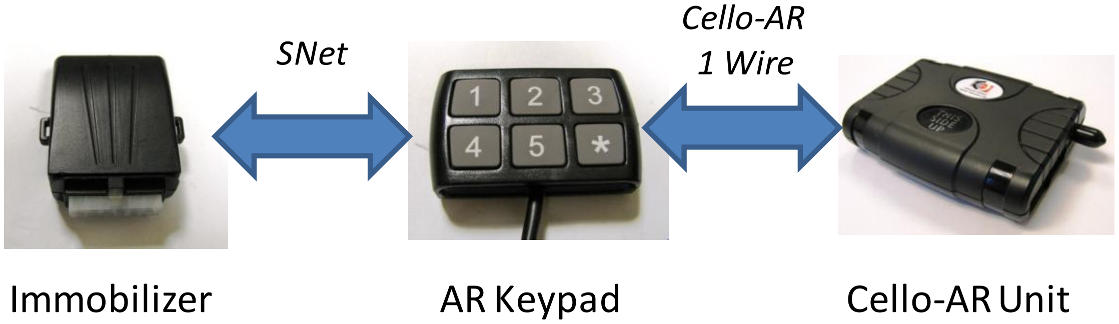
Feature	Activation Code	Confirmation indications (Number of beeps)
Restore default (means disabling engine on hotwire detection)	55555	5
Remove primary immobilizer pairing	51111	1
Remove secondary immobilizer pairing	52222	2
Remove wireless immobilizer pairing	53333	3
Activate pairing synchronization between keypad and Cello-AR	51124	4
Detecting Engine-on enabled	51112	2
Detecting Engine-on disabled	51113	3
Set passive arm time to 2 minutes	51423	1

Feature	Activation Code	Confirmation indications (Number of beeps)
Set passive arm time to 5 minutes	51424	2
Enable enter code on ignition-on	52323	1
Disable enter code on ignition-on	52324	2

6 Installation description

This section provides the required information for installing the components of the Cello-AR system. Further information regarding the Cello-AR installation is provided in CelloFamily Hardware Installation Guide.

6.1 Schematic diagram



6.2 Immobilizer Operation

The immobilizer utilizes 2 relays. The main relay (relay 1) is generally arranged in a normally open configuration which deactivates the engine. The secondary relay (relay 2) is generally arranged in a normally close configuration which secures engine operation during driving in transient periods. When in the Armed state and ignition is switched on, the immobilizer activates the secondary relay to deactivate the engine, and in the Disarmed state the immobilizer activates the main relay to ensure engine activation.

6.3 Immobilizer Pin out and Harness description

The immobilizer utilizes a 12 pins connector which is described in the table below:

Pin Number	Description
1	Power supply (+) 12/24(v) requires 3(A) fuse
2	Minus/Ground
3	Minus/Ground
4	Immobilizer status LED
5	Ignition
6	SNet
7	Normally Close 2

Pin Number	Description
8	Normally Open 2
9	Common 2
10	Normally Close 1
11	Normally Open 1
12	Common 1

The immobilizer is equipped with 1 meter, AWG 18, 12 wires harness connected to the immobilizer connector. The harness definition is described below.

Pin Number	Color	Printing	AWG	Length
1	Black	+12V	AWG18	1.5 m
2	Black	GND	AWG18	1 m
3	Black	GND	AWG18	1 m
4	Red	None (LED)	AWG18	1 m
5	Black	IGN	AWG18	1 m
6	Black	SNET	AWG18	1 m
7	Black	NC2	AWG18	1 m
8	Black	NO2	AWG18	1 m
9	Black	COM2	AWG18	1 m
10	Black	NC1	AWG18	1 m
11	Black	NO1	AWG18	1 m
12	Black	COM1	AWG18	1 m

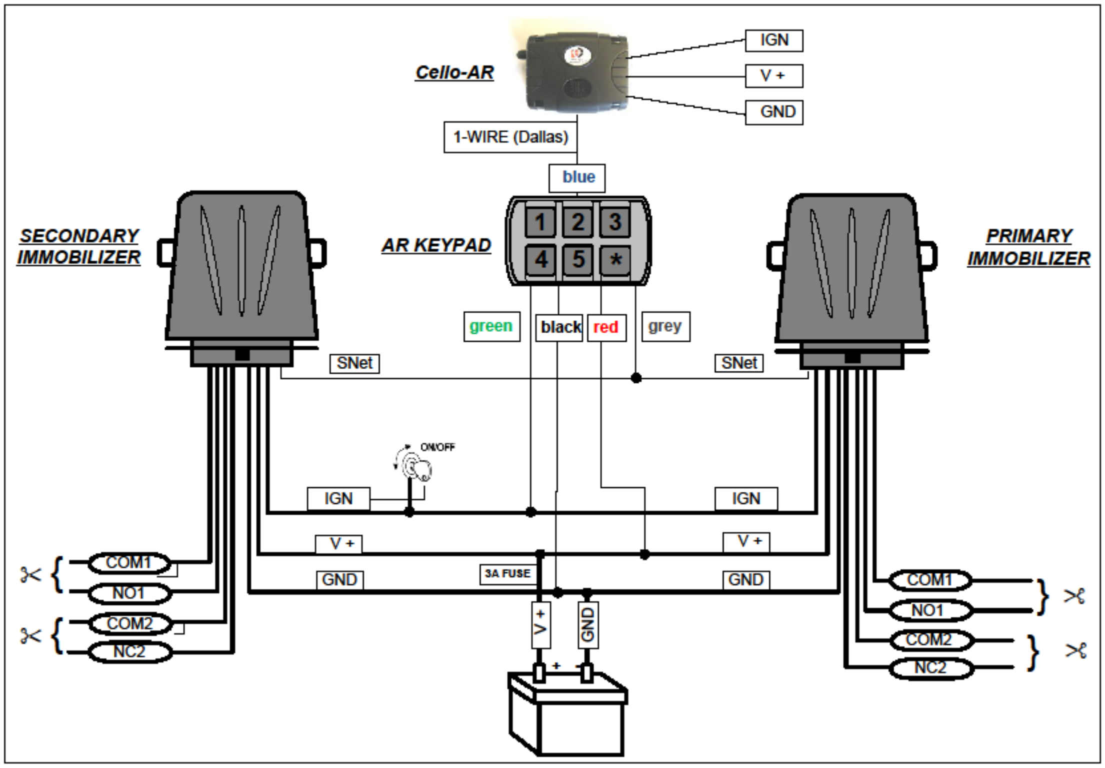
6.4 Keypad wiring table

Pin Number	Color	Description

Pin Number	Color	Description
1	Red	Power supply (+) 12/24(v)
2	Black	Minus/Ground
3	Green	Ignition
4	Gray	SNet
5	Blue	1-wire (Dallas)

6.5 Installation Diagram

The following diagram illustrates system installation according to the connection tables and recommendations described above.

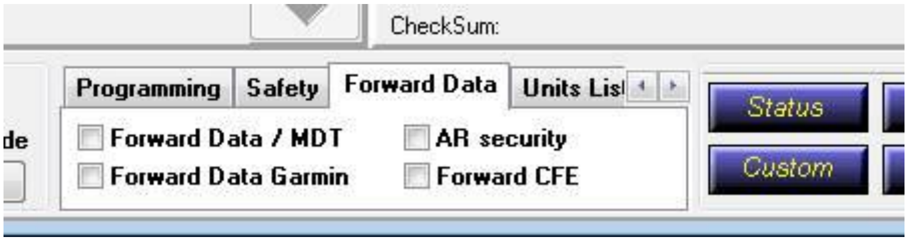


7 Evaluation

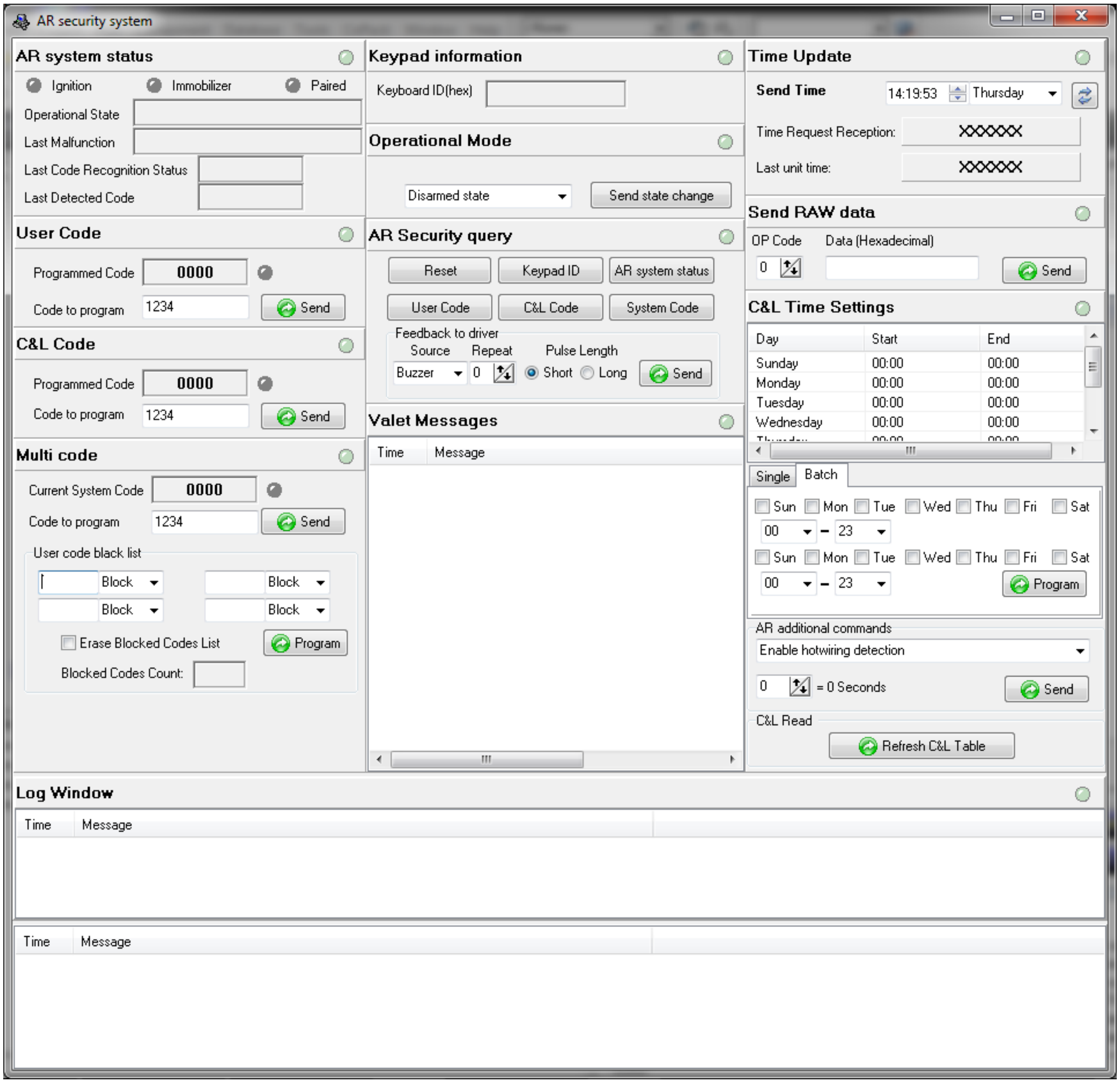
Evaluation of the Cello-AR is based on the Cello-F evaluation procedures. After the same evaluation environment required for the Cello-F is prepared, the Cello-AR system should be installed as described in the *Installation* section in the same environment.

The Communication Center has been modified and includes a special window for the evaluation of the special security capabilities of the Cello-AR security system.

In order to open the window, click on the **Forward Data** tab and then select the **AR Security** checkbox, as shown below.



The Cello-AR security system window is displayed, enabling you to evaluate the Cello-AR security system capabilities.



AR system status: Ignition, Immobilizer, Paired
Operational State
Last Malfunction
Last Code Recognition Status
Last Detected Code

Keyboard ID(hex)

Operational Mode: Disarmed state

User Code
Programmed Code 0000
Code to program 1234

C&L Code
Programmed Code 0000
Code to program 1234

Multi code
Current System Code 0000
Code to program 1234
User code black list: Block, Block, Block, Block
□ Erase Blocked Codes List
Blocked Codes Count:

Feedback to driver
Source: Buzzer
Repeat: 0
Pulse Length: ● Short ○ Long

Valet Messages

Time	Message

Time Update
Send Time 14:19:53 Thursday
Time Request Reception: XXXXXX
Last unit time: XXXXXX

Send RAW data
OP Code 0
Data (Hexadecimal)

C&L Time Settings

Day	Start	End
Sunday	00:00	00:00
Monday	00:00	00:00
Tuesday	00:00	00:00
Wednesday	00:00	00:00

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
00 – 23
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
00 – 23

AR additional commands
Enable hotwiring detection
0 = 0 Seconds

C&L Read

Log Window

Time	Message

Time	Message

8 Technical Specifications

This section includes technical specifications for the Cello-AR unit, the AR Keypad and the AR Immobilizer.

8.1 Cello-AR Technical Specifications

Communication	
GSM Modes	GPRS class 10, PDU SMS
Bands	Quad band: 850, 900, 1800, 1900MHz
Power Output	2W, 1W
SIM	Internal, replaceable, remote PIN code management
Antenna	Internal, quad band GSM antenna
Packet Data	TCP/IP, UDP/IP
SMS	PDU, text SMS for data forwarding
GPS	
Technology	Chipset: SiRFIII GSC3F/LP single chipset
Sensitivity (tracking)	-159dBm
Acquisition (normal)	Cold <42Sec, Warm<35Sec, Hot<1Sec
Antenna	On board, internal patch antenna Optional external Active antenna (2.85V ± 0.5%), automatic switching, standard SMA connector
Inputs and Outputs	
Inputs	1 internally pulled down input dedicated for ignition switch 3 internally pulled up general purpose inputs with assignable functionality and configurable polarity - 0V < Vil < 0.25V ; 0.25V < Vih ≤ 30V 2 configurable inputs capable to serve as: **Frequency counters - Configurable resolution;** Up to 5kHz input signal; Signal level (3V < Vin ≤ 30V) Accuracy ±2% **Analog inputs with variable resolution** - 8bit, adapted to 0-2.5V signal, resolution 20mV, accuracy ±20mV; 8bits, adapted to 0-30V signal, resolution 100mV, accuracy ±100mV **Discrete pulled up** - 0V < Vil < 0.25V; 0.25V < Vih ≤ 30V

	Discrete wet (configurable levels)
Outputs	5 general purpose open drain outputs (250mA max) with assignable functionality
Interfaces	
Voice Interface	Cellocator HF compliant Full duplex Echo cancelation Noise suppression Spy listening option Auto-answer option Volume control by single button or two buttons Distress voice call and plain call generation
COM (RS232) port	Selectable baud rate (9600 or 115000bps) - True RS232 levels; 8 bit; 1 Stop Bit No Parity MDT Interface Garmin™ Interface PSP™ (Car Alarm) Interface Cellocator Serial Protocol Transparent data mode Configuration Firmware upgrade
Debug port (RS232 out)	External Monitoring of Modem-CPU dialog
Debug port (RS232 out)	115000bps True RS232 levels 8 bit 1 Stop Bit No Parity
Deb1-Wire™ (Dallas port)	DS1990A compliant Driver management Car Alarm Authorization
Accelerometer	3D, 2g/8g range, <70mg resolution, I2C interface
Connectors	20pin Molex, Automotive SMA switch for optional external GPS Antenna

Power	
Input Voltage	7-32VDC
Average Current consumption	**Normal:** 40mA **Economic:** 23mA **Hibernation:** <2mA **Shipment (Off):** <20uA (Internal Battery)
Internal Battery	Li-Ion Polymer, 3.7V, 900mAh, rechargeable Embedded NTC for temperature controlled charging Operating Temperature: -20 (65% charge) to 60°C
Internal Battery	**Battery Monitoring:** Temperature (NTC) & voltage **Autonomy:** Up to 200 Tx @ 1Msg/min @ 25°C **Protections:** over current, overcharge and over discharge
Vehicle environment immunity	
Immunity	Compliant with ISO 7637 test level #4 (in accordance with e-mark directive)
Environment	
Temp, operating	-30°C to +70°C full performance -40°C to +85°C – degraded communication
Temp, storage	-40°C to +85°C
Humidity	95% non condensing
Protection	IP40
Vibration, Impact	ISO 16750
Mounting	Tie-wraps and/or two sided adhesive
Certifications	
FCC	Part 15 Subpart B, part 22/24 compliant
CE	CE EMC & R&TTE according to 89/336/EEC or 1999/5/EC CE Safety EN60950-1:2001+A11:2004 Automotive Directive 2004/104/EC (E-Mark)
IC	Industrial Canada
PTCRB	TRP, TIS, Spurious and harmonics emission
Dimensions & Weight	
Dimensions	91x73x23mm
Weight	110gr

8.2 AR Keypad Technical Specifications

Inputs and Outputs	
Inputs	1 internally pulled down input dedicated to ignition switch
Outputs	-
Interfaces	
SNet	Proprietary protocol for communication with the AR immobilizer
1-Wire™ (Dallas port)	Proprietary protocol for communication with the Cello-AR
LED	Built-in 6 LEDs used for visual indication to the user
Buzzer	Built in buzzer used for audible indication to the user
Connectors	5 pins SMD Headers 1.25mm
Power	
Input Voltage	7-32VDC
Average Current consumption	6 mA
Environment	
Temp. operating	-40 to+85°C
Dimensions & Weight	
Dimensions	91x73x23mm
Weight	110gr

8.3 AR Immobilizer Technical Specifications

Inputs and Outputs	
Inputs	1 internally pulled down input dedicated to ignition switch
Outputs	1 open drain output used for LED activation
Interfaces	
SNet	Proprietary protocol for communication with the AR-Keypad
Relay	Two relays utilize 3 contacts (common, normally open, normally closed)
Connectors	12 pins connector MINI-FIT

Power	
Input Voltage	7-32VDC
Average Current consumption	8 mA
Environment	
Temp, operating	-40 to +85°C
Dimensions & Weight	
Dimensions	91x73x23mm
Weight	110gr

8.4 AR Wireless Immobilizer Technical Specifications

Inputs and Outputs	
Inputs	1 Input-Ignition
Outputs	1 open drain output used for LED activation
Interfaces	
RF	RF receiver – 433.9 MHz; used for Snet communication with the AR-Keypad
Relay	Two relays utilize 3 contacts (common, normally open, normally closed)
Connectors	12 pins connector MINI-FIT
Power	
Input Voltage	7-32VDC
Average Current consumption	14 mA
Environment	
Temp, operating	-40…+85°C
Dimensions & Weight	
Dimensions	91x73x23mm
Weight	110gr