제 품 규 격 서

DR 품목

T200 Immobilizer System Specification

SPEC. # DPE-AE-IM159911S

	DTL				DWMC
	담 당	주 임	선 임	책 임	T200
결 재					

DAEWOO TELECOM LTD.

Revision	Description	DATE	Written By	Checked By
Revision A	First Preliminary based on DPI SPEC. # DPE-AE-IM159801S, revision G	00.12.11	C.G. Kwon	J.P. Ko
Revision B	-. Some LED status mode description has been corrected in Chap. 4.3.1 and Appendix B.	01.12.07	C.G. Kwon	J.H. Koo

Compliance Statement
THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES

Operating is subject to the following two conditions; (1) this device may not cause harmful interference, and (2) this device must accept ant interference received, including interference that may cause undesired operation.

CAUTION: Changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

1. Introduction

This document is the technical specification of the crypto transponder based Immobilizer System for the DWMC T200 car consisting of DTL Immobilizer Control Unit, IM800, (hereinafter Immobilizer or ICU) and Siemens Engine Control Module (ECM).

The purpose of the DTL Immobilizer System is to provide additional theft deterrence to the vehicle in which it is installed and to prevent it from being driven by unauthorized users. The verification of the user authorization is done by using an ignition key with integrated transponder.

The external LED displays the Immobilizer status and has an additional theft deterrence function.

To secure the communication, the status is exchanged between the Immobilizer and the ECM in a 5 bytes of encoded data.

These 5 bytes are composed by a mixture of random data and two types of fixed code :
- a Vehicle Model Identification Number : MIN
- a Vehicle specific Identification Number : VIN

The MIN is known from the first supply of the system.
The VIN is realized by ICU on the special order from the key coding (reading of transponder code and storing it as valid key code in Immobilizer EEPROM). A different random data is computed at each key transition.

All the immobilization communication between the ECM and ICU is made on K-line.

Due to the learning of the Vehicle specific Identification Number, both ICU and ECM can stay in 3 stable modes :
- Virgin mode (VIN not learnt)
- Learnt mode (VIN learnt)
- Neutral mode (for a new VIN learning)

Every Immobilizer system has one of 65,535 possible VIN-codes, which have to be equal to release the engine running. The definition of the VIN-code is executed by the Immobilizer.

The diagnosis of the Immobilizer is realized by the ALDL-function modes(refer to DPE-AE-IM159912S). They are realized by the Daewoo ALDL test equipment. To avoid manipulation of the usage of the test equipment, especially the use of the Key Coding procedure has to be protected against unauthorized use. So some critical services are only accessible by security access implemented in ICU diagnostic service, example for ‘read/reset ICU VIN-code’, ‘change to neutral mode’ and ‘authorize one additional key’, etc.

2 System Description

The T200 Immobilizer system consist of

- a maximum of 5 ignition keys with integrated transponder,
- the toroidal coil for energizing and reading the transponder mounted at the ignition lock,
- the Immobilizer control unit(ICU) with :
  - power supply (Term. 30),
  - ignition input circuit,
  - transponder modulation and demodulation unit,
  - uP with integrated EEPROM,
  - driver electronic for the external status LED,
  - serial data link hardware,
- the external status LED for displaying the Immobilizer status,
- the serial data link between Immobilizer and ECM and
- the serial data link between Immobilizer and Instrument Cluster(provision)
- the ECM itself.

The system is shown in Appendix A.

3 System Function

3.1 Immobilizing Function

- **Ignition ON Immobilizer :**

Turning on the ignition triggers the Immobilizer to read out the transponder data and to compare the read code with the valid key codes stored in the Immobilizer EEPROM. Until the end of transponder reading the Immobilizer is active state(cranking is not possible).

- In case of using a valid key, the internal relay is activated (cranking is possible) and the release message communication with the ECM takes place. The LED displays the Immobilizer status 'valid key'.

- In case of receiving no ECM request within the defined time-window the internal relay is deactivated(cranking is not possible). The LED displays the Immobilizer status 'valid key'.

- At the end of the TMPVDOUT delay the immobilization communication is stopped and the internal relay is deactivated and then the Immobilizer waits for a diagnosis request from the tester.

- In case of using a invalid key, 'no release answer' communication with the ECM takes place. The LED displays the Immobilizer status 'invalid key'.

- **Ignition ON ECM :**

After turning on the ignition the ECM will control the engine in a normal way for starting and running while waiting for a valid release response message from the Immobilizer (release time period).

- After receiving a response message including the information 'ICU in learnt mode' and the correct system VIN-code the ECM enters the release state, which allows to continue the running of the engine.

- After receiving a response message including the information 'ICU in learnt mode' and a wrong system VIN-code, the ECM does not send a new request and enters the blocked state, which causes the activation of the immobilization actions of the engine.

- If the ECM doesn't receive a response message within a defined time from beginning of the release time period and the ECM receives a no release answer, it enters the blocked state, which causes the activation of the immobilization actions of the engine.

- **Ignition OFF Immobilizer :**

  The inactive state of the Immobilizer(valid key / invalid key) ends with turning off the ignition.

- **Ignition OFF ECM :**

  The immobilizing state of the ECM (released/blocked) ends with turning off the ignition or with removing the battery voltage.

3.2 Functions for Protection against Manipulation

3.2.1 Vehicle Specific Identification Number(VIN)

The VIN-code is calculated by the Immobilizer using a random number generator.

The VIN-code is transmitted from the Immobilizer in the release message communication only in case of using an authorized key. Without an authorized key it is not possible to get the system VIN-code.

In case of ECM internal state is in virgin mode or neutral mode the ECM learns the system VIN-code automatically after receiving the first release response message.

To get a synchronized Immobilizer system (same VIN-codes in Immobilizer and ECM, authorized key) the function of Auto key learning procedure in the DWMC production line and the ALDL-test equipment has to be used for authorization of the keys (first Key Coding) in the field.
The usage of this test equipment is restricted to authorized persons.

4. System Components

4.1 Ignition Key with Integrated Transponder

4.1.1 Transponder Mounting

The transponder is placed invisible inside the ignition key. A second ignition key with integrated transponder on the bunch doesn't affect the reading process.

4.1.2 Transponder Function

The transponder is a read/write RF transponder. The transponder contains an implementation of a crypto-algorithm with 96 bits of user configurable secret-key contained in EEPROM. It also provides a unique device identification of 32bits that can never be modified as well as 30bits of freely programmable USER-MEMORY.
Bits 15 and 14 of word 1 are used as Lock-bits. The memory can only be accessed for writing or Erasing if these two bits have the contents "10" as when they are delivered.
The transponder transmits data to the transceiver(ICU) by modulating the amplitude of the electromagnetic field, and receives data and commands in a similar way.

4.1.3 Transponder Specification

*. Mechanical data

- Length of tube	13.3 +/- 0.4mm
- Diameter of tube	3.15 +/- 0.1mm
- Storage temperature	-40 to +85℃
- Operation temperature	-40 to +85℃

*. Electrical data

- Nominal resonance frequency	RF = 125kHz +/- 3kHz
- Bit Period	256us at RF = 125kHz
- Bitcoding	Manchester
- Modulation	AM

4.2 Toroidal Coil

4.2.1 Toroidal Coil Mounting

The toroidal coil is mounted at the ignition lock in front of the key barrel. It is integrated to the ICU housing package with a body of the coil to improve the performance of transponder reading and EMC.

4.2.2 Toroidal Coil Function

The toroidal coil and receiving coil inside the transponder built a transformer. During the reading process the coil induces energy into the transponder. The transponder charges the field and generates an amplitude modulated signal with the manchester coded data. This charge of the field is demodulated inside the Immobilizer.

4.2.3 Electrical Spec. of Toroidal Coil

- Operating temperature	-40℃ to +80℃	DR 특성
- Turns	80	
- Inductance(not on ignition lock)	407uH +/- 2% measured at 120kHz	DR 특성
- Inductance(on the ignition lock)	360 ± 10 μH measured at 120kHz	DR 특성
- DC resistance	4.8ohm +/- 5%	
- Cu-wire(diameter)	0.20mm	

4.2.4 Toroidal Coil Driver

The Immobilizer contains the coil driver hardware for direct connection of the toroidal coil.

4.3 Status LED

An external LED displays the Immobilizer system status. The Immobilizer contains the LED driver hardware for direct connection of one LED.

4.3.1 Status LED Modes

Mode	Status LED	Immobilizer System status	Note
Mode A	Blinking (f = 1Hz) Duty cycle 1 : 7	Immobilizer active	-. Ignition OFF -. Auto Key Learning is enable
Mode B	Blinking (f = 1Hz) Duty cycle 7 : 1	Immobilizer active	-. Ignition ON -. Invalid key detected or invalid learnt mode -. Learnt or Virgin mode
Mode C	OFF	Immobilizer inactive	-. Ignition ON -. Valid key detected -. Learnt mode
Mode C	OFF	Immobilizer active	-. Ignition OFF -. Any ICU status except in case of Mode A
Mode C	OFF	Learning in progress	-. Ignition OFF or ON -. Learning non successful or key yet learnt
Mode D	ON	Immobilizer active	-. Ignition ON -. Transponder doesn't detected
Mode E	Blinking (f = 0.5Hz) Duty cycle 5 : 5	Immobilizer active	-. Ignition ON -. Virgin state -. Entry to the Auto key learning
Mode F	Blinking (f = 1Hz) Duty cycle 5 : 5	Immobilizer active	-. Ignition ON -. VIN-code/MIN-code are different between ICU and ECM in learnt state
Mode G	Blinking(f = 2Hz) Duty cycle 5 : 5	Learning in progress	-. Ignition ON -. Auto learning of first key is successful
Mode H	Blinking(f = 4Hz) Duty cycle 5 : 5	Learning in progress	-. Ignition ON -. Auto learning of second key is successful

4.4 Immobilizer Electronic Control Unit (ICU)

4.4.1 Tasks

The function of the Immobilizer System is shared between the ICU and the ECM.
The tasks of the Immobilizer Electronic Control Unit(ICU) are :

- Reading of the input information 'Ignition ON/OFF'.
- Controlling the states LED.
- Controlling the transponder read/write process (modulation, demodulation, decoding, comparison of the read code with the codes of the valid keys).
- Communication with the ECM after ignition ON (receiving of the ECM-request and transmission of release message).
- Controlling the internal relay to connect 510ohm pull-up resistor or not.
- Special functions for calculation and handling of the VIN-code.
- Communication with the ALDL-test equipment. Main functions are the Key Coding procedure, the VIN-code handling and the support for system test functions.
- Handling of the software watchdog.
- Realization of functions for reducing the power consumption(cyclic wake up).
- Message encryption

4.4.2 Function

4.4.2.1 Normal Operation

- In the active mode of Immobilizer(engine off, ignition turned off) the status LED turned OFF as Mode C.

- When ignition is turned on, the system wakes up and tries to read out the transponder. The timing for all system is defined in the chapter 5.

- In case of the detection of a valid key, the release message communication with the ECM takes place. The status LED displays the Immobilizer state 'valid key' as Mode C. The maximum duration of the release message communication is restricted to a calibration time TMPVDOUT. This value must be defined until fixing of the Immobilizer software.

  - After receiving request message including the information 'ECM in virgin mode' and 'ECM in neutral mode' the ICU will send response message 'ICU in learnt mode' and will change to the inactive mode.
    The status LED is turned off.

  - After receiving request message including the information 'ECM in learnt mode' and the correct VIN-code, the ICU will send response message 'ICU in learnt mode' and will change to inactive mode. The status LED is turned off.

  - After receiving request message including the information 'ECM in learnt mode' and incorrect VIN-code, the ICU will send response message 'no release answer' and will change to active mode. The status LED displays the Immobilizer state 'different VIN-code'. And then in order to crank a vehicle the ICU should be changed to neutral mode by Tester equipment(change to neutral mode).

  - In case of no request from the ECM is received within the defined time TMPVDOUT, the Immobilizer stays in the active mode. The status LED is still displaying the Immobilizer state 'valid key'.

- In case of the detection of a invalid key, the ICU will send response message 'no release answer' and will change to active mode.
  The status LED displays the Immobilizer state 'invalid key'.

- After turning off the ignition (ignition OFF detection similar to the ECM ignition OFF detection), the Immobilizer changes to the active mode. The status LED is turned off as Mode C.

4.4.2.2 ALDL-mode

During ignition ON the Immobilizer ALDL-mode can be activated with one of the defined Immobilizer ALDL-Function modes.
Until the deactivation with the ALDL Function Mode 'Stop Communication Service' or detection of a time-out the Immobilizer stays in the ALDL mode. Cyclic transmissions of ALDL-function modes (same as Tester Present service) keep the Immobilizer in the ALDL-mode. The normal operation of the system (reading of transponder after turning ignition on, communication with the ECM, blinking of the status LED) is disabled during ALDL-mode.

- The status LED is turned off during ALDL-mode.
- The Immobilizer will answer all correct messages, which are defined as Immobilizer messages.
- Activation of ALDL-Mode after TMPVDOUT time delay may not cause a bus collision.

4.4.2.3 VIN-code Handling

The VIN-code is stored in the Immobilizer uP-EEPROM. At the end of the electronic unit production line the Immobilizer VIN-code has to be erased. The erased VIN-code(=0FFFFh) enables the VIN-code calculation procedure of the Immobilizer. The VIN-code can only be erased with the special Immobilizer ALDL-function 'Reset Immobilizer VIN-code'. It is not possible to change the VIN-code with the standard Key Coding procedure. The VIN-code can be read with the diagnostic function 'Read VIN-code service' and 'Read ICU & ECM mode service' for external comparison with the ECM VIN-code.

The VIN-code is a two byte random value in the range from 0000h to 0FFFFh. The VIN-code is fix for one car, but it has 65,535 variations in field. The value 0FFFFh is reserved to enable the VIN-code calculation procedure.

If the VIN-code calculation procedure is enabled, the first Key Coding procedure(normally the Key Coding procedure at DWMC production line) is followed by the VIN-code calculation procedure. The new VIN-code is transmitted to the ECM via the release message communication during the first starting with a valid key. The system timing in this case is the same as in case of the normal use of a valid key.

4.4.2.4 Calibration Parameter

- TMPVDOUT :
  It represents the maximum duration of the release message communication between the ECM and the ICU. The timer starts with detection of Ignition on. On the ECM side the time allowed to the Immo. Function is limited to a maximum value C_MAX_DLY_ACT_IMOB(typical value 768ms) which starts with the end of Tini time.
  If no request from ECM was received during limited time, TMPVDOUT, the release message communication is finished.

  - Timeout = TMPVDOUT * 100 ms
  - Calibration range =
    10 . . TMPVDOUT . . 254
    1 sec . . Timeout . . 25.4 sec
  - Default value
    TMPVDOUT = 20
    Timeout = 2 sec
  - EEPROM address TMPVDOUT = 31h

4.4.3 Connector for the ICU

The Immobilizer has two connectors. The terminal function is shown in the following table:

Terminal No	Function	Type
A1	Ignition (Term. 15)	Input
A2	Battery Power (Term. 30)	Power
A3	Serial data link(Instrument Cluster) - provision	Bidirectional data
A4	Vehicle GND (Term. 31)	Power
A5	Serial data link(ALDL Tester)	Bidirectional data
A6	Serial data link(ECM)	Bidirectional data
A7	External Status LED	Output

4.4.4 General Specification

Test item	Contents
Nominal voltage	12V
Test voltage	13.5V +/- 0.1V
Operating voltage	8 - 16 V
Undervoltage protection	Reset if U < 6V
Overvoltage protection	18V+/-0.1V 1hr, 24V 2min
Reverse battery protection	-13V+/-0.1V, 2min
Standby current	< 3mA (by using mask controller)
Operation current	< 200mA
Storage temperature range	-40℃ to +85℃
Operating temperature range	-40℃ to +80℃
Installation position	Passenger compartment
Resonance capacitance	adjusted to the toroidal coil
Outputs	All outputs are short circuit protected
LED driver current Ipeak	3.3 mA

4.4.5 Environmental Test Specification

Test Items	Contents
Rapid change of temperature test	According to EDS-T-5426 20 cycles -40℃ to +80℃ 30sec recovery time / 1h duration
Endurance test (Change of temperature test)	According to EDS-T-5426 -40℃ to +80℃ 12h per cycle (7h at +80℃ / 1h at –40℃) 50,000 cycles(5sec : ON, 5sec : OFF)
Frost test	According to EDS-T-5426 -20℃ 95% humidity 8 hours
Humidity test	According to EDS-T-5426 +40℃ 95% humidity 250 hours

Dust test	According to EDS-T-5426 Agitation : 5 sec each cycle Duration : 20 minute(1 cycle) 8 hours
Vibration test	According to EDS-T-5426 Duration : 8 hours each axis Frequency & Acceleration : 25Hz – 4.34G/Hz 1000Hz – 0.1G/Hz Total acceleration : 2G
Drop test	According to EDS-T-5426 Height : 1m Ground : concrete surface 2 shocks each direction (6 total)
EMC	
Functional Status Classifications : class C according to GM9100P	
Transients	EDS-T-5011
Load dump	EDS-T-5011
EMI test	EDS-T-5524
EMS test	EDS-T-5512 : Bulk Current Injection EDS-T-5514 : Magnetic Immunity EDS-T-5006 : Sinusoidal Burst
ESD test	EDS-T-5005

4.5 Engine Control Module(ECM)

4.5.1 Function Definition

The purpose of the immobilization function, in the ECM, is to immobilize the vehicle if the information received from the ICU are not recognized as the correct information.
That means after, when the ECM reset or, if a Key-Off/Key-On transition occurs, the ECM will read the status from the ICU : Is the engine authorized to keep on running or not?

All the immobilization communication between the ECM and ICU is made on the K-line.
Due to the learning of the VIN, both ICU and the ECM can stay in 3 stable modes.

To auto-protect the system, the time allowed to the immobilization function is limited to a maximum value C_MAX_DLY_ACT_IMOB which represents the maximum duration of the communication between the ECM and the ICU.

4.5.2 System states

At the first mounting of the ECM on the car, depending on a configuration calibration value, the ECM can be placed in Virgin mode or No-Immobilizer mode.

The customer calibration flag(LV_IMOB) indicates if the immobilizer option is installed on the vehicle.
Two cases are possible :

-. The customer calibration LV_IMOB is set to 1, then ECM enters in Virgin mode.
-. The customer calibration LV_IMOB is set to 0, then the ECM enters in No-Immobilizer mode.

4.5.2.1 ECM in Virgin Mode

In this mode, the ECM knows only the model vehicle identifier code.
The VIN code stored in non-volatile memory is 0FFFFh. The engine can be locked/unlocked.
ECM requests to ICU the VIN number. As soon as the ECM receives two correct consecutive communication frames with the same VIN code the ECM learns it. The VIN code will be stored in non-volatile memory instead of 0FFFFh at the end of power latch phase. ECM enters in Learnt mode.

4.5.2.2 ECM in Learnt Mode

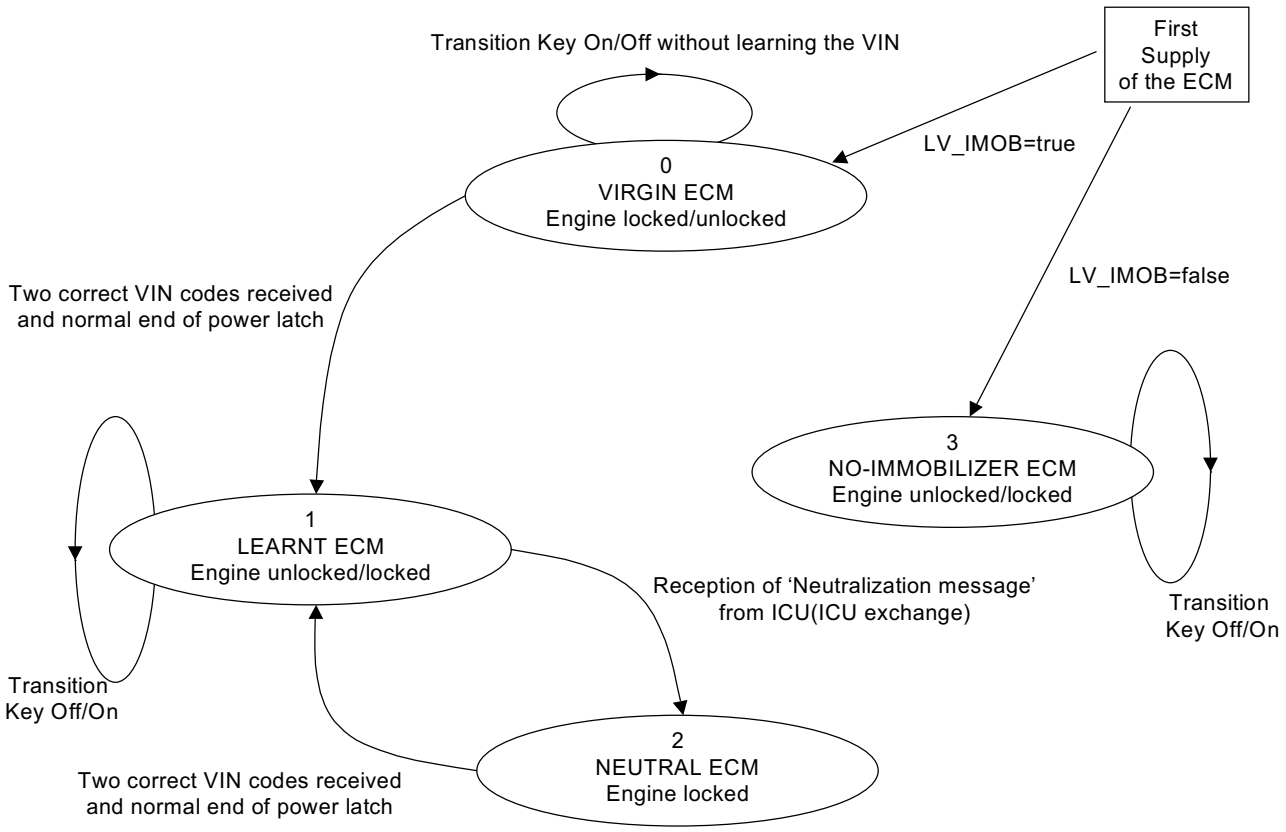
In such a state, ECM checks on every communication, the correct encoding of the ICU. If the code received is not correct, then the vehicle is immobilized.
The coded 5 bytes of data emitted by ECM are a mixture of MIN code and random bytes.
The coded 5 bytes of data emitted by ICU are a mixture of VIN code and random bytes.

4.5.2.3 ECM in Neutral Mode

This mode is a special intermediate mode, used for ICU replacement or immobilizer option installation. ECM requests to ICU the VIN number. As soon as the ECM receives two correct consecutive communication frames with the same VIN code the ECM learns it. The VIN code will be stored in non-volatile memory instead of 0FFFFh at the end of power latch phase. ECM enters in Learnt mode.

4.5.2.4 ECM in No-Immobilizer Mode

In this mode, the ECM will allow engine to run but if an ICU message is seen on the K-line, ECM is locked. The purpose is to avoid vehicle to be stolen by replacing ECM in Learnt mode by another one in No-Immobilizer mode.
The Immobilizer option cannot be added in the vehicle, even using the Scan Tool mode.
ECM is definitely in the No-Immobilizer mode.



4.6 Serial Data Link between Immobilizer and ECM

4.6.1 Electrical Specification

The exchange of the immobilization status between ECM and ICU is made on the current K line.

This configuration prescribes on the K line, a communication with physical addressing by the Tester at the diagnosis connector, as a real ISO 14230-1 K line. The only constraint is during the Immobilizer initialization, ICU and ECM cannot be addressed by the Tester for diagnosis.

The communication system consists basically out of two electronic units (Immobilizer and ECM). Depending on the car equipment other electronic units(transmission control) may be connected to the communication system. For realization of ALDL-functions the test equipment has to be connected to the serial data link through isolated connector pin A5 in the ICU.
In normal working state during communication between ICU and ECM the internal relay is activated and then the 510Ω pull-up resistor is connected to the Vbat(This resistor shall be included in the ICU). Because the K-line is disconnected by internal relay during normal communication time it may not cause a bus collision.
After the end of normal communication the internal relay is deactivated. The 510Ω pull-up resistor is disconnected to the K-line and then the serial data link of K-line is connected to the ICU and ECM data link through the internal relay.

4.6.2 Protocol Specification

Because of the special function ‘release message communication’ the protocol specification for the communication on the serial data bus has to be distinguished in different cases:

- Protocol specification during the time of release message communication:

  - The Immobilizer is defined as Slave. The ECM is defined as Master. The release message communication between Immobilizer and ECM is defined as special function in Immobilizer and ECM.
  - Other electronic units are defined as Remote.
  - The activation of ALDL-mode during the time is not allowed, it may not cause a bus collision.

- Protocol specification outside the time of release message communication:

  - The Immobilizer is defined as Remote.
  - The ECM is defined as Remote.
  - Other electronic units are defined as Remote.

- Protocol specification during ALDL-function

- The Immobilizer is defined as Remote.
- The ECM is defined as Remote.
- Other electronic units are defined as Remote.
- The test equipment is defined as Master.
  All communication is done via ALDL-function modes.

4.7 Serial Link between Immobilizer and Instrument Cluster(provision)

#TBD

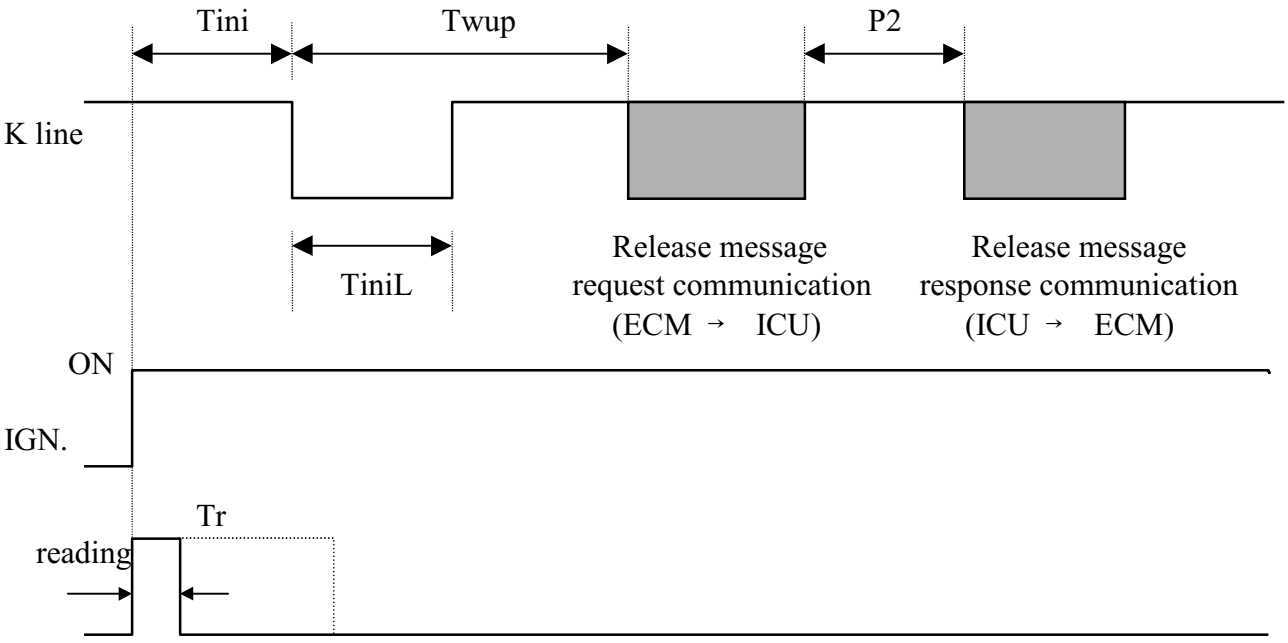
5 Communication Protocol

5.1 Communication Format

Baudrate	:	10400 Baud +/- 2%
Communication type	:	Point to point transmission in two directions between Immobilizer and ECM
Byteformat	:	1 start-, 8 data-, 1 stop bit
Bitformat	:	Non-Return-to Zero

5.2 Initialization of Communication

After Ignition on , the engine management system(ECM) will send a Wake Up Pattern (Wup) on K line after the initialization time Tini and will start the release message communication.



With :

Tini >= 510ms (This delay take account of Immo. constraint)

49 ms ≤ Twup ≤ 51 ms

39 ms ≤ TiniL ≤ 41 ms (low phase at the beginning)

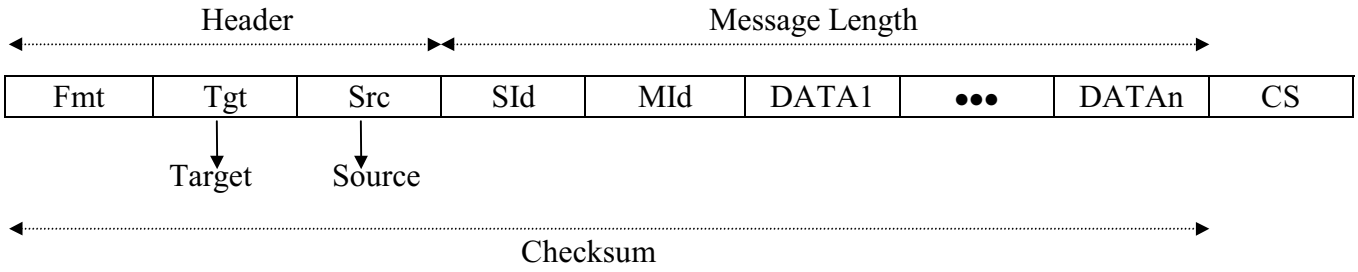
250 ms ≤ Tr ≤ 750 ms (transponder reading time)

During Tini, K-line must be on a high level.

P2 : Time between end of ECM request and start of an Immobilizer response

The ICU must constantly be in a position to detect a Wup since the interruption and re-initialization of the communication also takes place via the Wup in the event of an error.

5.3 Frame Structure

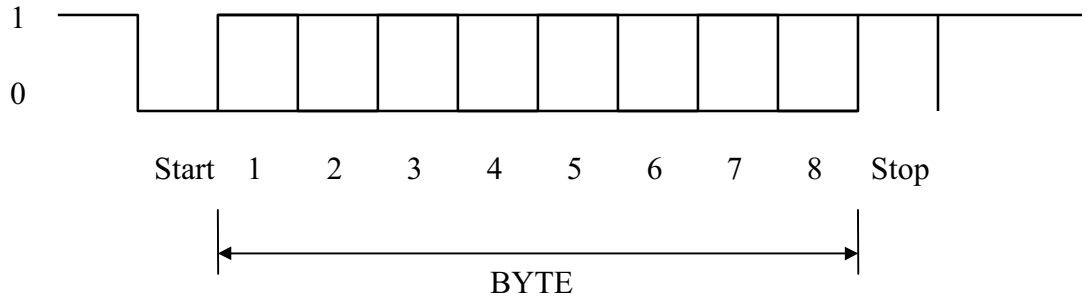


Byte #	Parameter Name	Hex value
1	Fmt : Message Length	8x
2	Tgt : Target	See header paragraph
3	Src : Source	See header paragraph
4	SId : Service Identifier	67 / 27
5	MId : Message Identifier	03 → 0E
6	Data byte 1 (MIN)	69
7	Data byte 2 (VIN high byte)	xx
8	Data byte 3 (VIN low byte)	xx
9	Data byte 4 (RND high byte)	xx
10	Data byte 5 (RND low byte)	xx
11	CS	xx

To secure the communication, the message is always encoded before transmission by the ECM to the ICU or by the ICU to the ECM, the methods of computation are confidential and described in Appendix C. The encoded 5 bytes are composed by a mixture of random data and two types of fixed code which are MIN and VIN. A different random data is computed at each communication by ECM.

5.3.1 Byte Structure

The structure of the Header, Data and Checksum bytes is as follows.



- Header

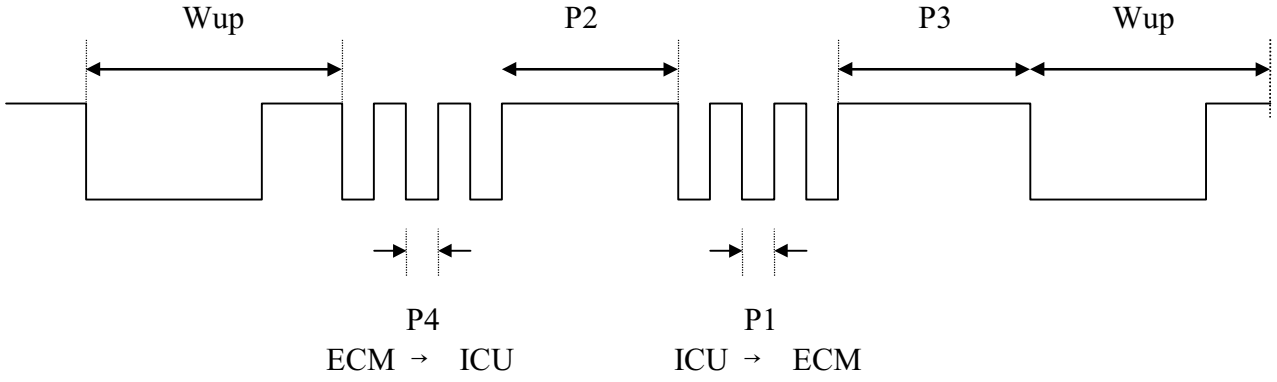
The following normalized values are used :

ECM	17h
Transmission	18h - 1Fh
Immo	C7h
DIAG tool	F0h

- Checksum Byte

The checksum byte(CS) inserted at the end of the message block is defined as the simple 8bit sum series of all bytes in the message excluding the checksum.

5.4 Message Timing



P1 : Inter byte time for Immobilizer request
P2 : Time between end of ECM request and start of an Immobilizer response

P3 : Time between end of Immobilizer response and start of an ECM new request (in case of incorrect answer received)
P4 : Inter byte time for ECM request

with :

0 ms ≤ P1 ≤ 5 ms
2 ms ≤ P2 ≤ 20 ms
2 ms ≤ P3 ≤ 20 ms
0 ms ≤ P4 ≤ 5 ms

Remark :
To secure the communication a Wup pattern will be sent before each ECM message.

DR 특성

5.5 Normal Mode Protocol

5.5.1 Normal Mode Communication Description

- In case of detection of a valid key the Immobilizer will wait for the wake-up pattern and request message from the ECM until the time window is reached or until the correct request from ECM is received. In case of detection of an invalid key, the Immobilizer will execute the 'No release answer' message communication.

- In a time window after turning on the ignition the serial data link is reserved for release message communication between Immobilizer and ECM.

5.5.2 System States

At the first mounting of the Immobilizer(ICU) on the car, the ICU in virgin mode and will stay in this mode until a request of specific vehicle code learning VIN from tech-1(tester).

As soon as the ICU receives the order(key coding procedure), it will learn the VIN-code and should keep this normal learnt mode in the field.

For special reason (ECM or ICU exchange) the ICU is able to be changed to neutral mode by tester equipment(Tech-1) and then the ICU may ask to the ECM to change to the neutral mode in order to allow the learning of a new VIN code.

5.5.3 Exchange of Immobilization Status

Services

All messages sent by the ECM will use the SId 67h.
All messages sent by the ICU will use the SId 27h.

Messages

- **ECM Messages**

See description of the 5bytes of data in the Release message.

MId = 03h	request for Immo. Status : ECM in virgin mode
MId = 05h	request for Immo. Status : ECM in neutral mode
MId = 07h	request for Immo. Status : ECM in learnt mode

- **ICU Messages**

See description of the 5bytes of data in the Release message.

MId = 04h	Immo. Status : No release answer - All ICU mode
MId = 06h	Immo. Status : Do not learn - ICU in virgin mode
MId = 08h	Immo. Status : Release answer - ICU in learnt mode
MId = 0Ah	Request for ECM : Neutralize - ICU in neutral mode

5.5.4 Release Message

5.5.4.1 ECM in Virgin Mode

Message from ECM : Mid = 03h

Source : ECM
Destination : Immobilizer
Message repeat : Every (50+61)ms until ICU response received or time-out

87h	C7h	17h	67h	03h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

Note : 00 00h = VIN empty

Response from ICU : Mid = 04h (no release answer)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	04h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = resend VIN value of the request message
RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation

Response from ICU : Mid = 06h (ICU is in virgin mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	06h	69h	00h	00h	RND #1	RND #2	CS

RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation (if long previous key ON)
Possible engine operation (if short previous key ON)

Response from ICU : Mid = 08h (ICU is in learnt mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	08h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = VIN-code of ICU
RND #1, #2 = resend RND value of the request message
Another request is sent and if the second VIN code received is the same than the first, the VIN code is memorized. If the second VIN is different the two VIN codes received are lost and another request is sent.
Answer considered as positive : Possible engine operation

Response from ICU : Mid = 0Ah (ICU is in neutral mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	0Ah	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = resend VIN value of the request message
RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation

5.5.4.2 ECM in Learnt Mode

Message from ECM : Mid = 07h

Source : ECM
Destination : Immobilizer
Message repeat : Every (50+61)ms until ICU response received or time-out

87h	C7h	17h	67h	07h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

Response from ICU : Mid = 04h (no release answer)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	04h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = resend VIN value of the request message
RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation

Response from ICU : Mid = 06h (ICU is in virgin mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	06h	69h	00h	00h	RND #1	RND #2	CS

RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation

Response from ICU : Mid = 08h (ICU is in learnt mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	08h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = if received VIN-code is different, ICU will send 'No release answer' and LED blinking state is Mode F(5 : 5) .
= if received VIN-code is same, VIN #1 and #2 are VIN-code of ICU.
RND #1, #2 = resend RND value of the request message
Answer considered as positive : Possible engine operation (if received VIN-code is same)

Response from ICU : Mid = 0Ah (ICU is in neutral mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	0Ah	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = resend VIN value of the request message
RND #1, #2 = resend RND value of the request message
After response of neutral mode the ICU state is changed to learnt mode.
ECM state change to neutral mode.
Answer considered as negative : No possible engine operation

5.5.4.3 ECM in Neutral Mode

Message from ECM : Mid = 05h

Source : ECM
Destination : Immobilizer
Message repeat : Every (50+61)ms until ICU response received or time-out

87h	C7h	17h	67h	05h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

Response from ICU : Mid = 04h (no release answer)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	04h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = resend VIN value of the request message
RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation

Response from ICU : Mid = 06h (ICU is in virgin mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	06h	69h	00h	00h	RND #1	RND #2	CS

RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation (long previous key ON)
Possible engine operation (short previous key ON)

Response from ICU : Mid = 08h (ICU is in learnt mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	08h	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = VIN #1 and #2 are VIN-code of ICU.
RND #1, #2 = resend RND value of the request message
Another request is sent and if the second VIN code received is the same than the first, the VIN code is memorized. If the second VIN is different the two VIN codes received are lost and another request is sent.
Answer considered as positive : Possible engine operation

Response from ICU : Mid = 0Ah (ICU is in neutral mode)

Source : Immobilizer
Destination : ECM
Response delay : < 20ms

87h	17h	C7h	27h	0Ah	69h	VIN #1	VIN #2	RND #1	RND #2	CS

VIN #1, #2 = resend VIN value of the request message
RND #1, #2 = resend RND value of the request message
Answer considered as negative : No possible engine operation

6 Special System Functions

6.1 Key Coding Procedure

The Key Coding procedure is executed by the test equipment. It is supported by two Immobilizer ALDL-function modes :

- The ALDL-function Mode 'Delete all key codes' deletes all Key Code memory locations in the Immobilizer EEPROM. After execution of this function a maximum of 5 keys can be authorized to the Immobilizer.

- The ALDL-function Mode 'Authorize one additional key' tries to read out the code of the actual inserted key and write it into the vacant key code memory location. This function is only executed successful if the ignition is turned on (to guarantee the correct location of the transponder according to the coil).

The authorization of a lost key can be deleted only by authorizing the remained keys as new set of keys.

All messages of Key Coding procedure are Immobilizer messages and doesn't affect the ECM. During the Key Coding procedure it is necessary to change the keys, if more than one key has to be authorized. Turning off the ignition has the effect the ECM pulls down the serial data link at the end of the turn-off delay. The ALDL-test equipment has to react correct in this case.

The test equipment software should be realized with the aim, that the whole Key Coding procedure for all keys, which the user wants to authorize, is executed automatically without additional user inputs on the terminal.

6.1.1 Key Coding on Production Line in DWMC

All memory locations for key data and the Immobilizer VIN-code has been deleted at the end of Immobilizer electronic unit production line.
The ECM VIN-code has been set to a value 0000h at ECM electronic production line.

The function 'Auto key learning procedure' as shown in Appendix B is repeated until two keys of this car are known to the system.
When two key learning is finished successfully, then the status LED is blinking as Mode H(duty cycle 5:5, 4Hz). After the end of Key Coding procedure the user has to turn on the ignition with one of the authorized keys to execute the ECM VIN-code learning procedure. After this the engine can be started with one of the authorized keys.

6.1.2 Key Coding of additional Keys in Field

The test equipment is connected to the ALDL-line. The function 'Authorize one additional key' is repeated until all additional keys of this car are known to the system. The user may terminate the procedure.

6.1.3 Key Coding of a New Set of Keys in Field

The test equipment is connected to the ALDL-line. All memory locations for key data must be deleted with the function 'Delete all key data'. The function 'Authorize one additional key' is repeated until all new keys of this car are known to the system.

7 Diagnostic Services

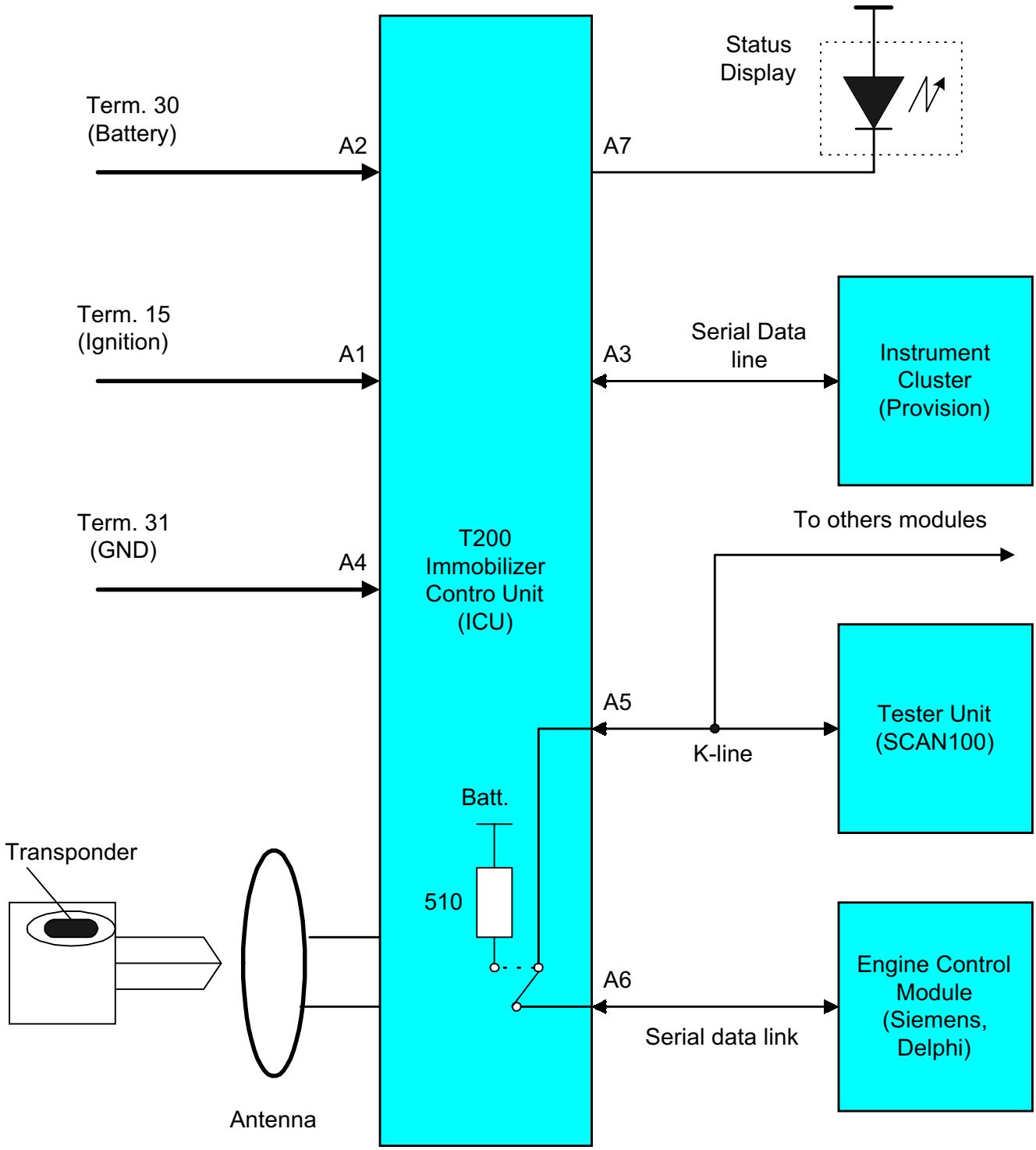
DR 특성

7.1 Summary of Nominal Diagnostic Services

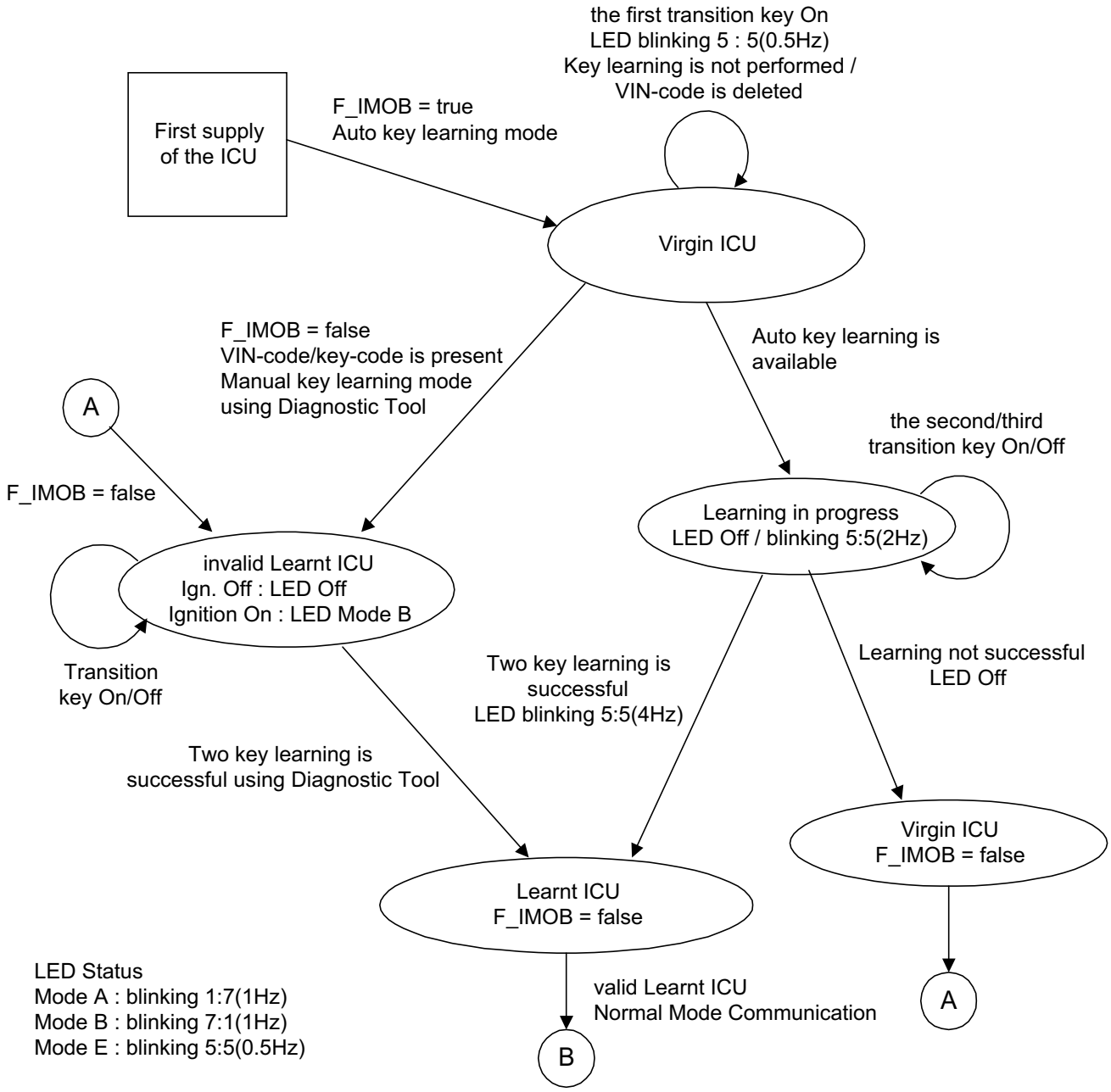
The following overview shows all implemented diagnostic services of Immobilizer. The detailed message format is described in spec.#DPE-AE-IM159912S.

ICU supported services	Request Value	Sub-Request Value	Security Required	Comments
Start Communication	81	-	-	standard diagnostic communication services
Stop Communication	82	-	-	
Access Timing Parameters	83	-	-	
Tester Present	3E	-	-	
Start Diagnostic Session	10	-	-	
Stop Diagnostic Session	20	-	-	
Security Access	27	-	-	
Reset Immobilizer VIN-code	A7	20	YES	normal diagnostic services
Read Immobilizer VIN-code	A7	21	YES	
Change to Neutral Mode	A7	22	YES	
Read ICU and ECM mode	A7	24	YES	
Read Allowed Address	A7	31	-	
Write Allowed EEPROM Address	A7	32	-	
Read Port	A7	33	-	
Read Key Code	A7	34	YES	
Delete All Key Codes	A7	35	YES	
Authorize one additional key	A7	36	YES	
Write port	A7	38	-	
Read Magic User Memory	A7	40	YES	
Magic Authentication	A7	41	YES	
Magic Write Word	A7	42	YES	

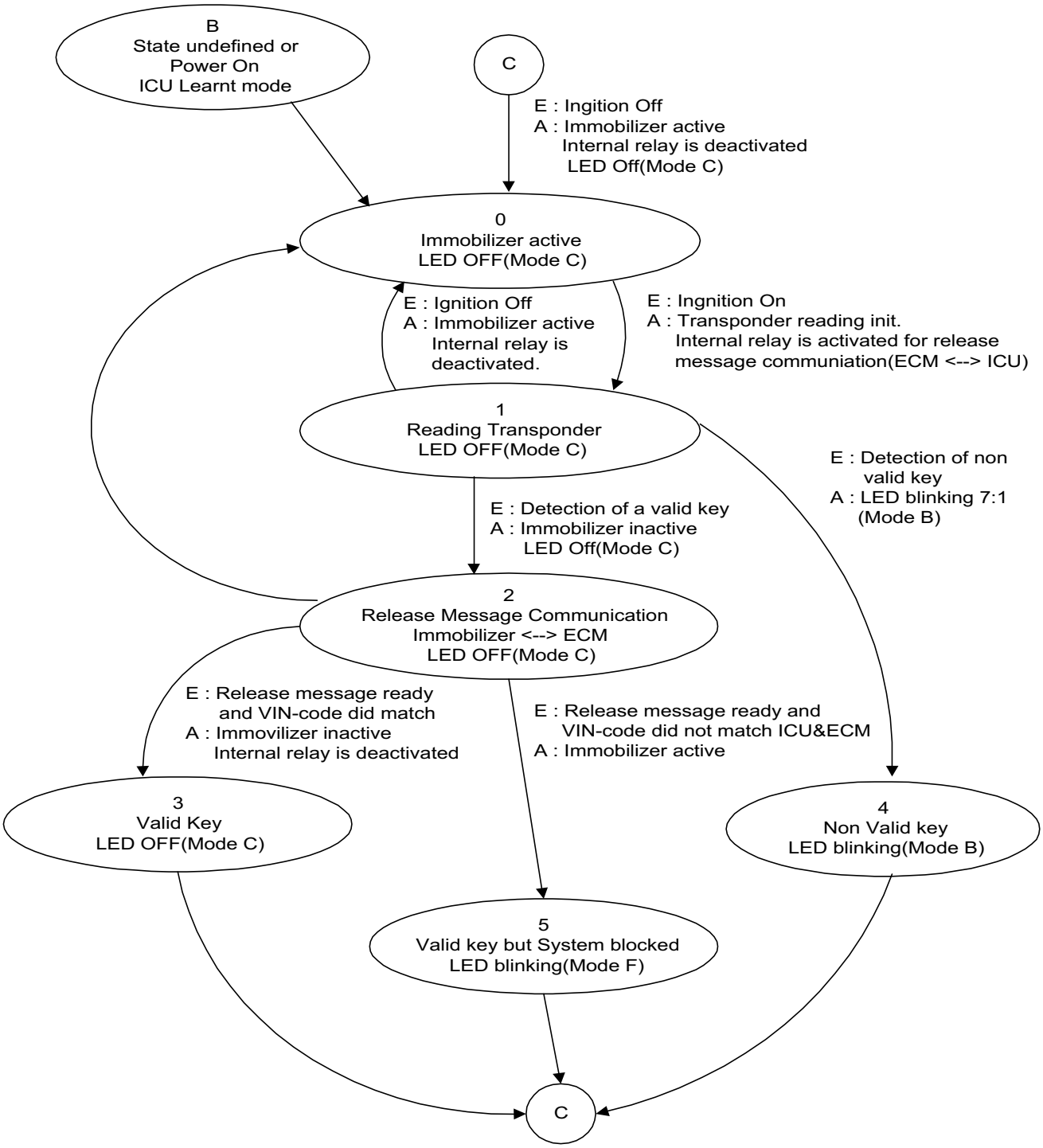
Appendix A. Block Diagram of Immobilizer System



Appendix B. State Transition Diagram of Immobilizer System(Virgin mode)



Appendix C. State Transition Diagram of Immobilizer System(Learnt mode)



E : Event which causes the change of the state
A : Action which performed with changing the state

Appendix D. Encryption Computation

The message is always encoded before transmission by both systems, the methods of computation are confidential.

1. 5 bytes of transmitting message data
   MIN : VIN_H : VIN_L : RND_H : RND_L

2. Store VIN_H with the result of exclusive-or VIN_H and RND_H.
   $VIN_H = VIN_H \oplus RND_H$

3. Store VIN_L with the result of exclusive-or VIN_L and RND_L.
   $VIN_L = VIN_L \oplus RND_L$

4. $i = 0$

5. Divide Key Byte(MIN) into 2 nibbles.
   $K_i = (K_H, K_L)$

6. Check MSB of RND_H(random byte high).
   IF MSB = '0' THEN $K_i = (!K_H, !K_L)$; ! $\rightarrow$ 1's complement
   ELSE IF MSB = '1' THEN $K_i = (K_L, K_H)$

7. Store RND_L with the result of exclusive-or RND_H and Key Byte.
   Store RND_H with RND_L.
   $R_{L\_i+1} = R_{H\_i} \oplus Ki$
   $R_{H\_i+1} = R_{L\_i}$

8. Rotate left Key Byte(1 bit).
   $C \leftarrow K_{MSB} \ldots K_{LSB} \leftarrow C$

9. $i = i + 1$

10. If $i < N(N=7)$ then repeat 6 to 9 steps,
    else stop the encoding computation.

Appendix E. Decryption Computation

The message received is always decoded by both systems, the methods of computation are confidential.

1. 5 bytes of received message data
   MIN(Key Byte) : VIN_H : VIN_L : RND_H : RND_L

1. i = N (N=7)

2. Divide Key Byte(MIN) into 2 nibbles.
   K_i = (K_H, K_L)

3. Rotate right Key Byte (1 bit).
   C → K_{MSB} . . . K_{LSB} → C

4. Store RND_H with the result of exclusive-or RND_L and Key Byte.
   Store RND_L with RND_H.
   R_{H_i-1} = $R_{L\_i} \oplus K_i$, R_{L_i-1} = R_{H_i}

5. Check MSB of RND_H(random byte high).
   IF MSB = '0' THEN K_i = (!K_H, !K_L) ; ! → 1's complement
   ELSE IF MSB = '1' THEN K_i = (K_L, K_H)

6. i = i - 1

7. If i > 0 then repeat 3 to 7 steps.

8. If K_0 != 69h(MIN) then go to 10 step (computation error).

9. Store VIN_L with the result of exclusive-or VIN_L and RND_L.
   Store VIN_H with the result of exclusive-or VIN_H and RND_H.
   VIN_L = $VIN_L \oplus RND_L$
   VIN_H = $VIN_H \oplus RND_H$

10. stop decoding computation.