IMMOBILIZER

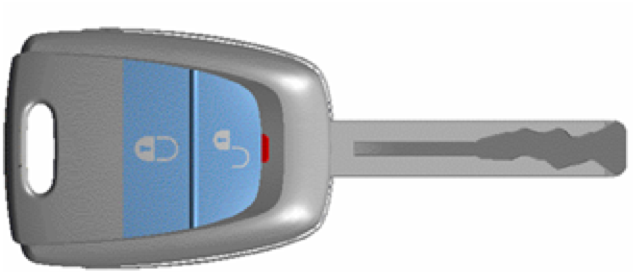
(SMARTRA 3)

Published by
Chonan Technical Service Training Center

Objectives	To know SMARTRA 3 type immobilizer system. To understand the diagnosis method of Immobilizer system. To understand defferent thing between SMARTRA and SMARTRA 3

The SMARTRA 3 immobilizer system is applied for ED. SMARTRA 3 type immobilzer system is almost same as SMARTRA type. Only different thing is information of transponder is stored to SMARTRA 3 unit. So, this system include SMARTRA neutralize and teaching mode for SMARTRA.

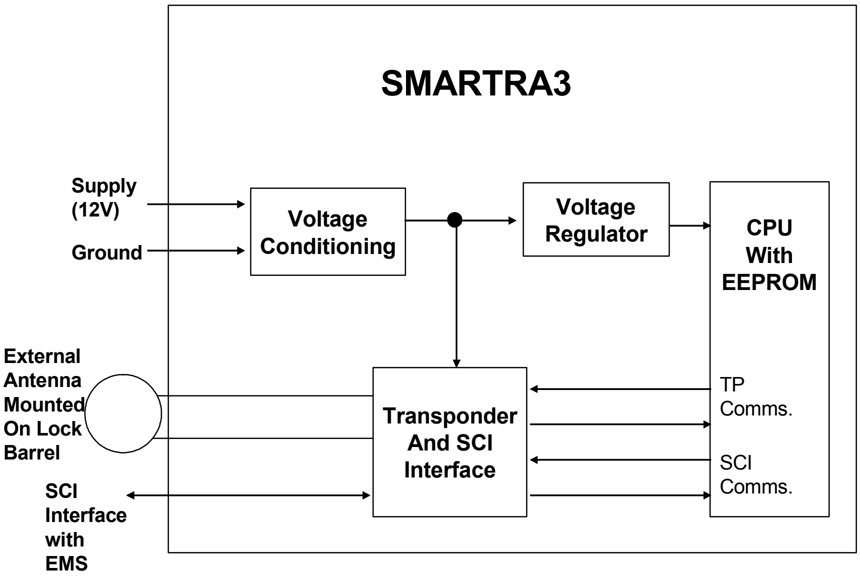
This manual will explain more detail information about SMRATRA 3 immobilizer system.



1. Intorduction

ED is applied SMARTRA 3 type immobilizer irrespective of engine type.

The immobilizer system consists of a transponder inside the key knob, the encoded SMARTRA3 unit /key and the ECM can decode the secret code stored in the SMARTRA3. The ECM communicates the encoded messages to the SMARTRA3 via a dedicated communication line and confirms the key with the SMARTRA3.



SMARTRA Block Diagram

All pins are protected against short to supply and ground. It is preferable to have all SMARTRA3 lines directly connected to the ECM to reduce noise interference.

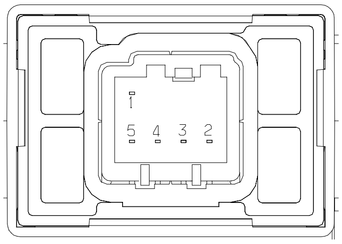
PIN 1 : Antenna coil (+)

PIN 2 : Communications Line

PIN 3 : Supply (12V)

PIN 4 : Grund

PIN 5 :Antenna coil (-)



2. component

SYSTEM OVERVIEW

The immobilizer system consists of the ECM, the SMARTRA3 and ignition keys with built-in transponder.
The ECM carries out the check of ignition key by special encryption algorithm with SMARTRA3 and Transponder.

When IGN On, the ECM executes the key Authentication after SMARTRA3 authentication.
The Engine can be started in case of the success in SMARTRA3 and key authentication.

The ECM and the SMARTRA3 communicate by dedicated line. During this communication of ECM and SMARTRA3 the K line of ECM cannot be used for communication. The ECM controls the communication either to SMARTRA3 or to other devices (e.g. Hi-scan pro or GDS) on K line by switching of a multiplexer and specific communication procedures. The multiplexer is a part of ECM H/W.

The SMARTRA3 carries out the communication with the built-in transponder of the ignition key. This wireless communication runs by RF (Radio frequency of 125 kHz). The SMARTRA3 is mounted at the ignition lock close to the antenna coil for RF transmission and receiving. The RF signal from the transponder received by the antenna coil is converted into messages for serial communication by the SMARTRA3 device. And the received messages from the ECM are converted into the RF signal, which is transmitted, to the transponder by antenna.

The SMATRA3 executes the encryption algorithm and transmits the encryption result. And SMARTRA3 is in charge of relaying from ECM to Transponder.

The SMARTRA3 is teached in key Teaching process and stores the encrypted code in memory inside SMARTRA3. This encrypted code is used in encryption algorithm between ECM and SMARTRA3 and to neutralize the SMARTRA3. When SMARTRA3 is neutral, old encrypted code and informations of transponder are deleted.
New encrypted code can be stored in Neutral SMARTRA3.

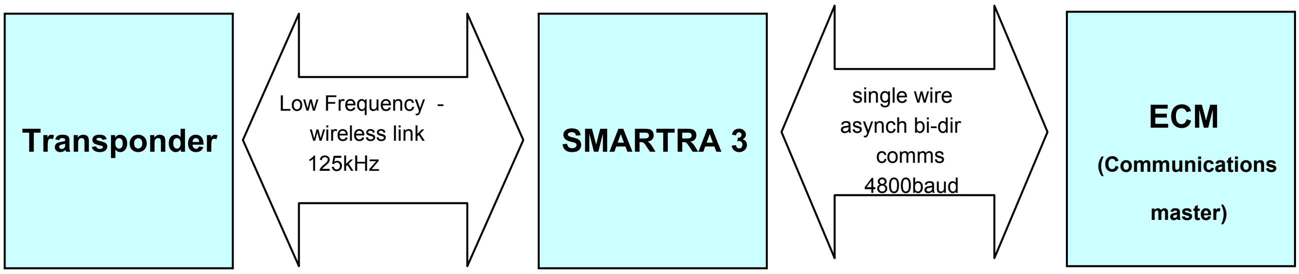
During the key teaching procedure the transponder will be programmed with vehicle specific data. The vehicle specific data are written into the transponder memory. The write procedure is unique; therefore the content of transponder can never be modified or changed. The data are a string of 9 bytes defined

by vehicle manufacturer. The transponder memory is split into two strings called authenticator (6 bytes) and key password (3 bytes).
After this programming the transponder memory is locked and the data cannot be read or changed respectively. The transponder status changes from „virgin“ to „learnt“.

Additionally every transponder includes a unique IDE (Identifier number) of 32 bit. Unique means that the IDE of all transponder is different from each other. The IDE is programmed by the transponder manufacturer and is a read-only value.

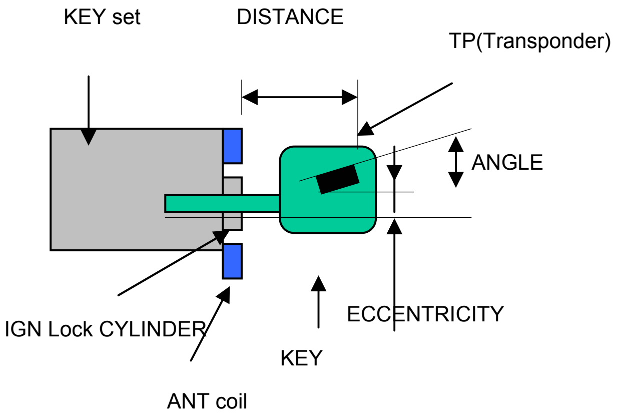
The authenticator and the key password are not transferred from ECM to transponder or vice versa. Only the results from the encryption algorithm are transferred. It is almost impossible to calculate the vehicle specific data from the encryption result.

For teaching of keys and special purposes the ECM is connected to the tester device. This can be the manufacturer’s service tester, which is in use at service station. The protocol of communication is KWP2000 at the K line of ECM.

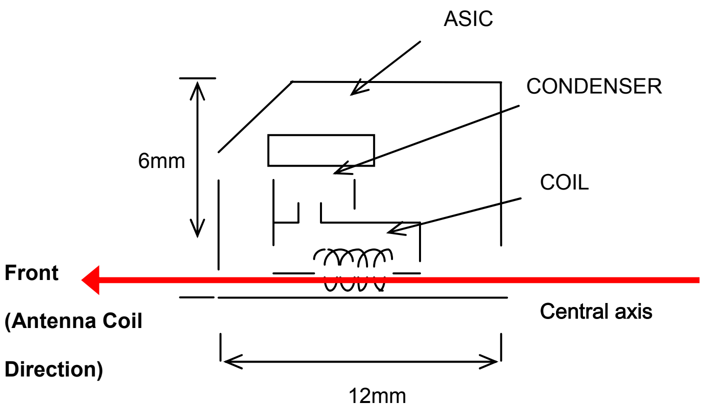

Transponder
Low Frequency - wireless link 125kHz
SMARTRA 3
single wire asynch bi-dir comms 4800baud
ECM
(Communications master)

2.1 TRANSPONDER

This part details the layout condition for transponder performance.



Definition for component



Structure for TP

* SPECIFICATION FOR TRANSPONDER LAYOUT

- DISTANCE: below 28mm
- ECCENTRICITY: below 3mm
- ANGLE: 3 degree

KEY STATUS about immobilizer is defined by GST.

The status of user password defines the possibility of limp home function.
After request from the tester the ECM sends the status information. This status is stored in the permanent memory (EEPROM or Flash etc.).

00 Not yet checked

The stauts is stored in permanent memory (EEPROM or Flash etc.) In case of not plausible data from this circuit the ECM can not check the key status.

01 Learnt

The key has been taught successfully.

02 Virgin

The key has not been taught successfully.

03 Invalid

The key registerd by another car.

2.2 SMARTRA 3

SMARTRA3 STATUS about immobilizer is defined by GST.

The status of user password defines the possibility of limp home function.
After request from the tester the ECM sends the status information. This status is stored in the permanent memory (EEPROM or Flash etc.).

00 Not yet checked

The stauts is stored in permanent memory (EEPROM or Flash etc.) In case of not plausible data from this circuit the ECM can not check the SMARTRA3 status.

01 Learnt

The encrypted code is stored in SMARTRA3.

02 Virgin

The encrypted code is not stored in SMARTRA3.

03 Neutral

By neutral command from GST (HI-SCAN Pro) this status can be set.
encrypted code is deleted from SMARTRA3.

04 Locked by timer

After a certain number of incorrect inputs the ECM is locked for one hour and no inputs are accepted during this time.

05 Invalid

In case that the encryption results from SMATRA is different from the encryption result calculated by ECM.

2.3 ECM

ECM STATUS about immobilizer is defined by GST.

The status of user password defines the possibility of limp home function.
After request from the tester the ECM sends the status information. This status is stored in the permanent memory (EEPROM or Flash etc.).

00 Not yet checked

The status is stored in permanent memory (EEPROM or Flash etc.). In case of not plausible data from this circuit the ECM cannot check the status.

01 Learnt

At least one key has been taught successfully.

02 Virgin

This is the status at the end of ECM production line before delivery to final customer

03 Neutral

By special command from tester (HI-SCAN Pro) this status can be set.
The vehicle password and key information are deleted.

04 Locked by timer

After a certain number of incorrect inputs the ECM is locked for one hour and no inputs are accepted during this time.

2.4 PIN CODE

The PIN codes (6 digits) of each vehicle are managed by KMC characteristic program.

These 6 digits are used in key teaching or ECM neutral, SMARTRA3 neutral and when the limp home password is losted.

The sequences of the PIN code storage are as follows.

1) Input the PIN code (6digits) into the diagnostic tester when key teaching process The diagnostic tester transmits the encrypted code to the ECM after converting the PIN code into encrypted code.
2) When the ECM gets the firtst key Teaching command , it transmits the SMARTRA3 Learnt command and encrypted code to the SMARTRA3
3) If the SMARTRA3 statue is virgin/neutral, the SMARTRA3 stores encrypted code in EEPROM and transmits the success message of the encrypted code storage. (If the SMARTRA3 is learnt, the SMARTRA3 compares encrypted code transmitted by the ECM with encrypted code stored in EEPROM and transmits the (in)correct encrypted code message to ECM)
4) If the SMARTRA3 is learnted normally or the encrypted code of the registered SMARTRA3 is same as the ECM, the ECM begins operation the Transponder Teaching.
5) If the Teaching of the first transponder, the ECM stores the encrypted code in its EEPROM and converts state into learnt state.

2.5 IMMOBILIZER SYSTEM TEACHING PROCEDURES

In the processing the teaching of immobilizer system, at first the ECM request the PIN code to the tester. The immobilizer teaching is possible when the status of ECM is “virgin” or “neutral”. After comparing PIN code stored in ECM with PIN code inputted from tester, if the result is same, the learnt ECM will start teaching the immobilizer system.

The teaching immobilizer procedure is comprised of the SMARTRA3 teaching and the key teaching.
If the ECM receives the key teaching message from diagnostic tester, it will teach the SMARTRA3 at first and then KEY.
After the first key teaching, it will omit the SMARTRA3 teaching from second key teaching and keep teaching another key.

If the SMARTRA3 is not taught normaly or taught by another vehicle, the ECM will terminate the communication and key teaching.

2.5.1 SMATRA3 TEACHING

The key teaching is done at End of Line of vehicle manufacturer, after replacing defective SMATRA3 at service station or for providing of additional keys to the vehicle owner.

The procedure starts with ECM request of vehicle specific data (encrypted code) from tester.
The SMATRA3 teaching is possible in case that the status of SMARTAR is “virgin” or “neutral “. In case that the SMARTRA3 is “learnt”, the SMARTRA3 will transmits the information whether PIN code inputted from tester is same as the PIN code in SMARTRA3.

The SMARTRA3 teaching is possible regardless of key status.

The SEK (Secrete Encryption key) is used in encrypted communication between SMARTRA3 and ECM. The SEK is made from PIN code inputted during SMARTRA3 teaching.
If the SMARTRA3 is learnt, the SEK will be stored in EEPROM. The ECM stores the SEK in EEPROM in case that one more key is taught validly.

If the PIN code inputted from ECM fail over 3 trials (3trials: continuously or_intermittently), the ECM will not accept the request of key teaching for an hour.
Disconnecting the battery or other manipulation cannot reduce this time. After the connecting of battery to ECM the timer starts again for one hour.

2.5.2 KEY TEACING PROCEDURES

The key teaching is done at End of Line of vehicle manufacturer, after replacing defective ECM at service station or for providing of additional keys to the vehicle owner.

The procedure starts with ECM request of PIN code to tester. The „virgin“ECM stores PIN code and the key teaching can be started. The „learnt“ECM compares PIN code from tester with the encypted code in transponder. If the data are correct, the key teaching can be started.

If wrong PIN code have been sent to ECM three times continuously or intermittently, the ECM will reject the request of key teaching for one hour. Disconnecting the battery or other manipulation cannot reduce this time. After connecting the battery the timer starts again for one hour. If the ECM has not backup power, this time can reduce in the IG condition.

The key teaching is done by ignition on with key and additional tester command. The ECM stores the relevant data in the permanent memory (EEPROM or Flash etc.) and in the transponder. Then the ECM runs the authentication for confirmation of teaching process. The successful programming is confirmed by message to tester.

If the key is already known to ECM from previous teaching the authentication will run and the permanent memory (EEPROM or Flash etc.) data are updated. There is no change of transponder content (this is impossible for learnt transponder).

The attempt of repeated teaching of a key, which has been taught already during the same teaching cycle, is recognized by ECM. The ECM rejects this key and a message is sent to the tester.

The ECM rejects invalid keys, which are presented for teaching. A message is sent to the tester. The key can be invalid due to faults of transponder or other reasons, which result into not successful programming of data. If the ECM detects different authenticators of transponder and ECM, the key is considered to be invalid.

The maximum number of taught keys is 8.

If the ECM status and the key status do not match for teaching of keys, the tester procedure will be stopped and DTC is stored at ECM.

☞ **Next key should be inserted with in 10 sec in key teaching procedure**

2.5.3 USER PASSWORD TEACHING PROCEDURE

The user password for limp home is taught at service station. The owner of the vehicle can define a number with 4 digits.
The user password teaching is only accepted by “learnt” ECM. Before first teaching of user password to ECM the status of this password is „virgin“. limp home function is impossible

The user password teaching is started by ignition on with a valid key(learnt key) and sending the user password by tester (choose menu “02 User password Teaching/changing“ on tester screen.
After successful teaching the status of user password changes from “virgin“to “learnt“.

The learnt user password can also be changed. This can be done if the user password status is „learnt“and the tester sends for authorization of access either the old user password. After correct authorization the ECM requests new user password. The status remains in „learnt“and the new user password will be valid for next limp home mode.

If wrong user passwords or wrong PIN code have been sent to ECM three times continuously or intermittently, the ECM will reject the request of password changing for one hour. Disconnecting the battery or other manipulation cannot reduce this time. After connecting the battery the timer starts again for one hour. If the ECM has not backup power, this time can reduce in the IG condition.(ex. Diesel ECM)

☞ User Password Teaching/Changing Condition:

- ECM STATUS: Learnt
- SMARTRA3 STAUS: Valid Learnt
- KEY STATUS: valid(Learnt) Key
- By Tester

☞ ECM Locked by Timer Condition:

- Input incorrect User Password (4 digits) or PIN Code (6 digits) 3 trials.

☞ Locked by Timer meanings: Locking of ECM

☞ Locked by Timer Release:

- Ignition ON ≥1 hour(Diesel only) or
- More than 1hour regardless of Ignition ON/OFF(Gasoline only)
Note. After 1 hour, ECM should reset incorrect data counter(PIN & User Password).

☞ ECM Locked by Timer Table

Function ECM	Engine Running			Teaching	
	Learnt(Invalid or Valid Key)	Limp home	Twice Ignition	Key	User password
Locked by Timer	No	No	No	No	No

The user password can be in the status as follows.

This status is stored in permanent memory (EEPROM or Flash etc.).

00 Not yet checked

The status is stored in permanent memory (EEPROM or Flash etc.).

In case of not plausible data from this circuit, the ECM cannot check the status.

01 Learnt

The password has been taught successfully to ECM.

02 Virgin

This is the status at the end of ECM production line before delivery to final customer.

03 Locked by timer

After a certain number of incorrect inputs the ECM is locked for one hour and no inputs are accepted during this time.

04 Teaching not accepted

This status is set if the ECM is in neutral of virgin status.

2.5.4 SMARTRA3 Neutral

The SMARTRA3 neutral function is possible through the diagnostic tester. When the the PIN code is inputted and the SMARTRA3 Neutral is requested by diagnostic tester, it is possible, regardless of the ECM status and the key status.

I.e. the ECM transmits the SMARTRA3 Neutral command to SMARTRA3 by order of the diagnostic tester.

2.6 LOCKING OF ECM

If engine shut off (ignition off by key) the ECM is locked from now on.
If the timer is more than 30sec without cranking in Ignition status “ON” by valid key,
ECM has to do new authentication if user attempts engine start.

In case of engine stalling about start of limp home the timing of ECM locking is as follows:

- Without ignition off there is the time limited by 30 senconds for repeated engine start, after ignition off the time for repeated engine start is limited to 8 sec.

- After elapsing this time new authentication is done or in case of limp home the input of user password is requested again.

2.7 UNLOCKING ECM

This is the release of fuel injection and ignition by ECM for successful start of the engine. The normal operation is with valid key. A key is valid after successful programming of vehicle specific data to the transponder and storing of relevant data of the transponder in the ECM / SMARTRA3.

Additionally there is a limp home function implemented to cover faults of transponder or SMARTRA3.

For special purposes during the vehicle manufacturing process the function „twice ignition on"is implemented. In this case, the status of ECM,SMARTRA3 and Transponder must be "Virgin".

For limphome mode and twice ignition**,** the unlocked status remains for the time (30sec)
After elapsing of timer the ECM is locked again. By using a valid key a new authentication runs after begin of cranking. In case of limp home and twice ignition new inputs are requested.

Immobilizer lamp control during ignition ON (No cranking) by valid key: 30sec

2.7.1 UNLOCKING WITH TRANSPONDER

This is the normal operation of the system in case of authorized using.

The main objective of the ECM immobilizer function is to determine whether the starting and running of the engine is enabled or not. For that, two ECM states are considered:

- *Locked* state: state in which the starting and running of the engine is disabled ; immobilizing actions are executed.
- *Unlocked* state: state in which the starting and running of the engine is enabled in a normal way.

At each ignition on transition, ECM is in unlocked state and it starts authentication procedure.

At first the ECM requests the TP IDE and transmits the Random Number to SMARTRA3.
SMARTRA3 response the TP IDE and encrypted Random Number to ECM.
ECM compares the Random Number responded from SMARTRA3 with its calculated Random Number.and after checking TP's unique IDE, if it is same as data inside ECM, the following authentication process will start.

The authenticator, the IDE and a Random Number are converted into the encrypted lock password and transferred to the transponder via the SMARTRA3. The transponder compares the data with its calculation result. If the results are equal, the transponder sends back the encrypted key password to ECM.

If this is equal to the calculation result of ECM, the ECM remains unlock state.

The unlocked ECM releases fuel injection and control of ignition.

The driver is informed about successful authentication by Immobilizer lamp at dashboard. The lamp is on after successful authentication until the detection of minimum engine speed for ECU operation (begin of engine cranking).

If user attempts engine start, After ignition ON by Valid Key, ECM is in unlock state and it starts re-authentication procedure.

Re-authentication procedure is same as authentication procedure at ignition on transition.

If the IDE is unknown or the calculation result from the transponder is different from the ECM calculation result, the ECM will be locked.

If the messages from SMARTRA3 are disturbed (e.g. by electromagnetic interference) and therefore the checksum of data is wrong, the authentication will be repeated 2 times additionally. After three attempts with fault the ECM will be locked and an error is stored. After the next ignition on the ECM is set into the limp home mode.

3 attempts must be finished within 1.5sec after authentication starts.

2.7.2 Limp home by GST (HI-SCAN)

If the ECM detects a fault of SMARTRA3 or transponder, the ECM will allow limp home function of immobilizer. Limp home is only possible if the user password (4 digits) has been taught to the ECM before. This password can be defined by vehicle owner and is programmed at the service station.

The ECM informs the driver about the limp home condition by blinking Immobilizer lamp. Then the user password can be sent to the ECM by tester menu.

Only if the ECM is in status „Key(TP) learnt“ and the user password status is „learnt“ and the user password is the correct one, the ECM is unlocked for 30 sec. The engine can only be started during this time. After elapsing of timer no engine start is possible.

If wrong user passwords have been sent to ECM three times, the ECM will reject the request of limp home for one hour. Disconnecting the battery or other manipulation cannot reduce this time. After the connecting of battery to ECM the timer starts again for one hour.

☞ **Limp Home Condition:**

- ECM Status PIN Code & User Password "Learnt",
- SMARTRA3 and Transponder error
- Input correct User Password(4) by GST or Key
after IMMO Lamp 5 Times blinking(1Hz/50%duty)
- Unlocking of ECM is allowed(up to 255 Times)

☞ **Unlocking Time of ECM: 30sec**

☞ **Unlocking Release Condition after Engine Running by Limp Home:**

IGN OFF ≥8sec

☞ **Unlocking time(30sec) resetting of ECM:**

- suddenly ENG STALL in Limp Home Mode
- IGN OFF ≤8sec in Limp Home Mode

☞ **IMMO Lamp Control : 30sec**

2.7.3 Limp home by Ignition key

The limp home can be activated also by the ignition key. The ECM informs the driver by blinking immobilizer lamp about the limp home condition. Then the input of user password to ECM can be done by special sequence of ignition on/off. The timing is described at attachment.

Only if the ECM is in status „learnt“ and the user password status is „learnt“ and the user password is the correct one, the ECM is unlocked for 30 seconds. The engine can be started during this time. After elapsing of timer no engine start is possible. After new input of user password, 30 seconds timer starts again.

2.7.4 TWICE IGNITION ON FUNCTION

This is a special function for engine start by vehicle manufacturer. The engine can be started for moving from the production line to an area where the key teaching is processed. This function is only perfomed in condition that ECM, SMARTRA3 and key are all Virgin status.

The engine can be started by the sequence

- Ignition on with no cranking,
- Ignition off,
- Ignition on with cranking within a time interval.

The following timing conditions have to be fulfilled for successful start:

- ECM, SMARTRA3 and key are all Vigin stauts.
- first ignition on more than 0.5sec and less than 1.5 sec
- ignition off time is limited by the minimum of 0.2 sec and the maximum of 1.5 sec
- ignition on

The numner of engine starts by "twice ignition on" is limited. The maximum value is defined by S/W constant. (Value is 32, regardless of cranking)

☞ **Twice Ignition ON Condition:** **- ECU & Key(TP) & SMATRA3 : Virgin only** **- 0.5sec ≤ First IGN ON ≤ 1.5sec** **- 0.2sec ≤ IGN OFF ≤ 1.5sec** **- Ignition ON**
☞ **Twice Maximun Value: 32 Times**
☞ **Unlocking Time Of ECM after Twice Ignition ON: 30sec**
☞ **The ECM is Instantly locked by IGN OFF after Twice Ignition**
☞ **IMMO Lamp Control: 30sec**

2.8 DIAGNOSIS OF IMMOBILIZER RELATED FAULTS.

The diagnosis monitors

- the communication between ECM and SMARTRA3,
- the function of SMARTRA3 and transponder and the data (stored at ECM) related to the immobilizer function.

Item	Description	DTC
Transponder Faults	1. Corrupted data from Transponder(TP) 2. More than one TP in the magnetic field 3. No TP(Key without TP) in the magnetic field	**P1693** TP No response Error, TP Invalid response
	1. TP not in the password mode 2. TP transport data has been changed	**P1674** TP status Error
	TP programming error	**P1675** TP Programming Error
SMARTRA 3 Faults	Antenna coil error	**P1691** Antenna Coil Error
	Communication line Error (Open/Short etc.)	**P1690** SMARTRA3 no response
	Invalid message from SMARTRA3 to ECM	**P1676** SMARTRA3 message error
	1.Virgin SMARTRA3 at Learnt ECM 2.Neutral SMARTRA3 at Learnt ECM 3.Incorect the Authetication of ECM and SMARTRA3 4. Locking of SMARTRA3.	**P169X** SMARTRA3 Authentication fail
Invalid Key	1. Virgin TP at ECM status "Learnt" 2. Learnt(Invalid) TP at ECM status "Learnt"	**P1696** TP Authentication fail
ECM internal permanent memory (EEPROM or Flash etc.)fault	ECM internal permanent memory	**P1695** ECM MEMORY Error
	Invalid write operation to permanent memory (EEPROM or Flash etc.)	
ECM Fault	1. Request from ECM is invalid (Protocol layer violation- Invalid request, check sum error etc.)	**P1694** ECM message Error
	Exceeding the maximum limit of Twice IGN ON(≥32 times)	**P1699** Twice Overtrial
Tester (HI-SCAN or GST etc.) fault	1. Request from Tester is Invalid (Protocol layer violation- Invalid request, check	**P1697** HI-SCAN Message Error

	sum error etc.)	
Others	Immobilizer Lamp error	**P1692** Immobilizer Lamp Error
	Non-immobilizer ECM in the immobilizer vehicle	**P1610** Non-Immobilizer-ECM connected to an Immobilizer

2.9 REPLACING OF IMMOBILIZER SYSTEM

2.9.1 REPLACING OF ECM

If the ECM is only replaced using an existing key and SMARTRA3, after replacing the “virgin” or “ neutral” ECM, reteacing is possible by key teaching mode of tester.

When the same PIN code used in existing vehicle is only inputted, the SMARTRA3 teaching and key teachings are possible.

The PIN code stored in SMARTRA3 can be deleted by the neutralization command. But the password stored in Transponder is not. After re-teaching all key taught before, they can be used.

2.9.2 NEUTRALISING OF ECM

The ECM can be set to the status „neutral“by tester.

Ignition key is inserted and after ignition on the ECM requests the PIN code from tester. The communication is performed by tester menu “04 Neutral Mode“. After successful receiving of data the ECM is neutralized.

The vehicle specific data have to be unchanged due to the unique programming of transponder. If data should be changed, new keys with virgin transponder are requested.

If wrong PIN code have been sent to ECM three times continuously or intermittently, the ECM will reject the request to enter neutral mode for one hour. Disconnecting the battery or other manipulation cannot reduce this time. After connecting the battery the timer starts again for one hour. If the ECM has not backup power, this time can reduce in the IG condition.(ex. Diesel ECM)

☞ **Neutralizing Setting Condition:**

In case of ECM Status “Learnt” regardless of User Password Virgin or Learnt, Input correct PIN Code by Tester

Function / ECM	Engine Running			Teaching	
	Learnt Key	Limp home	Twice Ignition	Key	User Password
Neutral	No	No	No	Yes	No

2.9.3 REPLACING OF SMARTRA 3

If the SMARTRA3 is only replaced using an existing key and ECM, after replacing the “virgin” or “ neutral” SMARTRA3, re-teaching is possible by key teaching mode of tester.

In this case, all existing key must be retaught.

If SMATRA3 is replaced to another one (used at other vehicle), it can only recycle in case of having same password before.

2.9.4 NEUTRALISING OF SMARTRA3

The SMARTRA3 can be set to the status „neutral“by tester.

Ignition key (regardlss of key status) is inserted and after IGN ON.

If receiving the correct PIN code from tester, SMARTRA3 can be neutralized.

The neutralization of SMARTRA3 is possible if PIN code is same as the value inputted by tester.

In case that the SMARTRA3 status is neutral, the ECM keeps the lock state. And the start is not possible by “twice ignition”.

In case of chaging the PIN code, new virgin transponder must be only used. And in case of virgin key, after teaching the key, it can be used.

If wrong PIN code have been sent to SMATRA3 three times continuously or intermittently, the SMATRA3 will reject the request to enter neutral mode for one hour. Disconnecting the battery or other manipulation cannot reduce this time. After connecting the battery the timer starts again for one hour.

☞ **Neutralizing Setting condition:**

- In case of SMARTRA3 status “Leartn”

- Input correct Pin code by tester

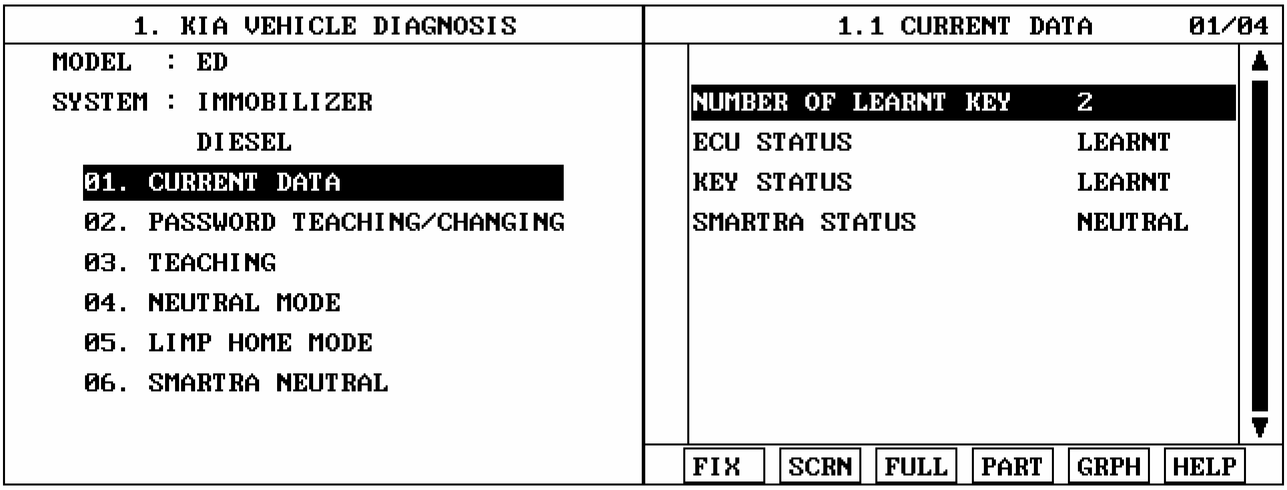
☞ **Neutralizing meaning:**

-PIN code & Information of transponder deletion

-Permission of New key teaching

Function SMARTRA3	Engine Running			Teaching	
	Learnt Key	Limp Home	Twice Ignition	Key	User Password
Neutral	No	Yes (ECM learnt)	No	Yes	No

3. GST (Hi-Scan) Menu



```
1. KIA VEHICLE DIAGNOSIS
 MODEL  : ED
 SYSTEM : IMMOBILIZER
          DIESEL
   01. CURRENT DATA
   02. PASSWORD TEACHING/CHANGING
   03. TEACHING
   04. NEUTRAL MODE
   05. LIMP HOME MODE
   06. SMARTRA NEUTRAL
```

```
1.1 CURRENT DATA      01/04

NUMBER OF LEARNT KEY     2
ECU STATUS               LEARNT
KEY STATUS               LEARNT
SMARTRA STATUS           NEUTRAL
```

4. Attachment : timing of limp home mode

•Normal Condition (No failure)

-Ignition on status (no engine running): 100 % duty (lamp on: 30 sec)

-As soon as detecting engine running: 0 % duty (lamp off)

•In case of failure (limphome)

-when user password (by key or Hi-scan) input is needed: 1 Hz 50 % duty (blinking) for 5 seconds

=> If there is a failure, as soon as ignition on, lamp has to blink for 5 seconds.

=> User has to input password after finishing lamp's blinking.

-After completing correct user-password input: 100 % duty (lamp on) during 30sec

⇨ During the input of user password by ignition key, lamp has to be operated according to the Ignition status.

⇨ During the input of user password by Hi-scan, lamp has to be off.

⇨ If time of 30ses has been elapsed without engine start, lamp has to be off and engine start is also prohibited.

⇨ If incorrect user password is inputted, when next ignition on (after power latch/after-run time), 50% duty blinking for 5seconds again for the request of correct password..

- As soon as detecting engine running: 0 % duty (lamp off)
- The user password by ignition key input procedure: refer to next page
- Engine can be stalled by miss-manipulation of clutch in case of M/T.
  If ignition key remains ON, as a safety function, during the engine running by user password (limphome), restart within 30 seconds has to be possible without input of password again**.**
  In this case, the timer starts just after the detection of engine stall.
  During that time, lamp has to be on.
- Engine can be start again in case of limphome mode without the new input of user password if users restart within 8(T7) seconds after ignition off.

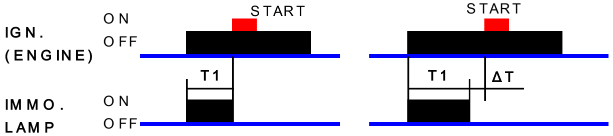
*Lamp on indicates the status engine is ready to start over 30sec.

*Lamp off indicates the status engine is running.

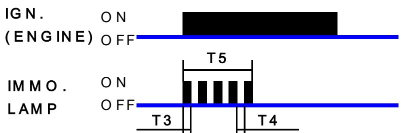
*Lamp blinking indicates the status user password input is needed because of uncertain failure.

Timing diagram

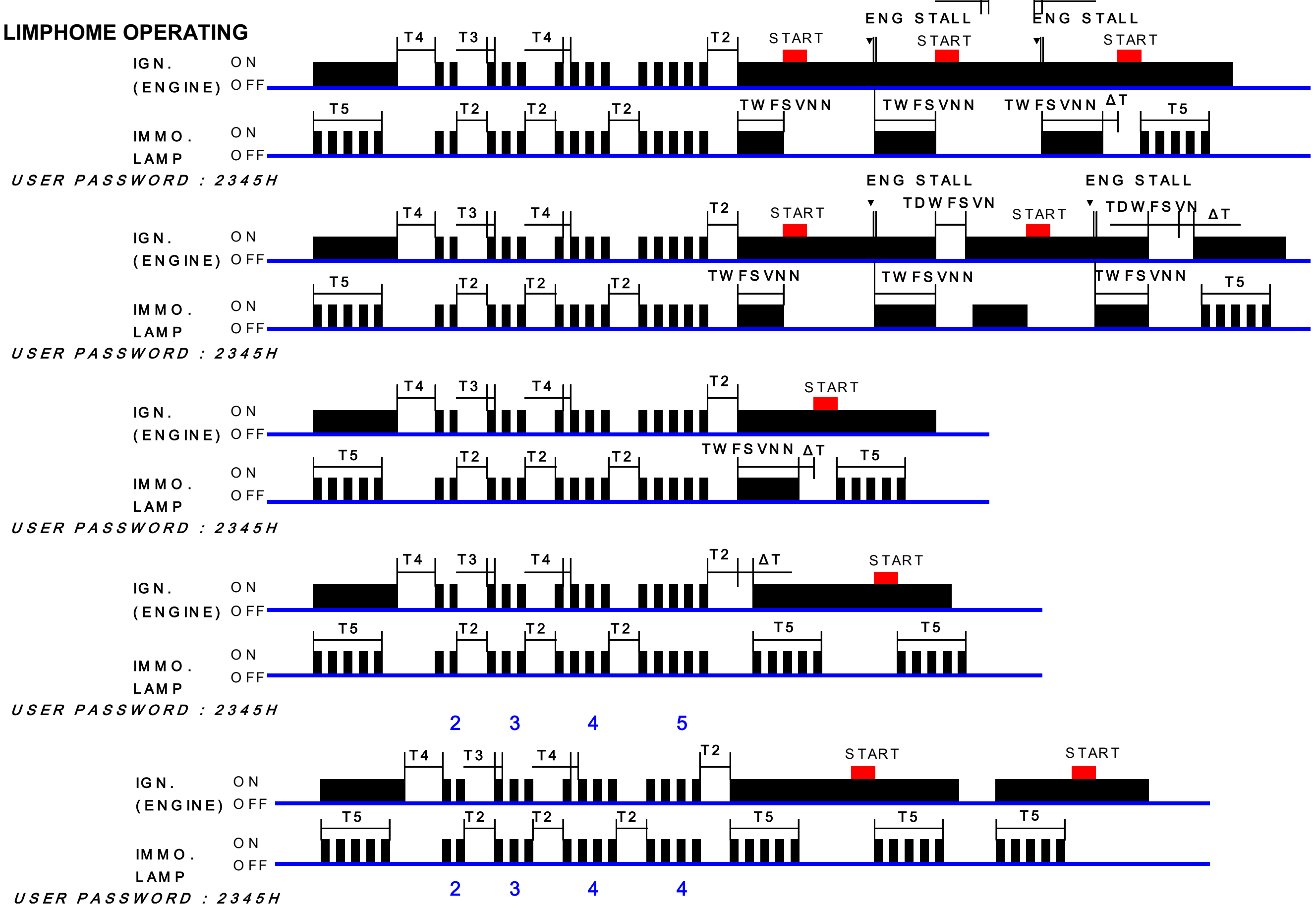
1. NORMAL CONDITION(NO FAILURE)



2. IN CASE OF FAILRE(LIMPHOME)



3. LIMPHOME OPERATING



NOTE :

T1 > 5sec
3sec < T2 < 10sec
0.2sec < T3 < 5 sec
0.2sec < T4 < 3sec
T5 = 5sec
T6 < 30sec
TDWFSVN = 8sec
TWFSVNN = 30sec
CODE "0" = IG.ON 10 TIMES