RQONE03795530_SIA_Base_Software_Suitable_to_Tasking_Compiler

Table of Contents

_Security_Immobiliser_Authority_for_Base_Software_Compatible_To_Tasking_Compiler

UNIQUE_DOORS_ID :	PS-328001_1
Object Type :	STKH_HEADER

Abbreviation

VCU - Vehicle Control Unit
IBU - Integrated Body Control Unit
VIN - Vehicle Specific Identification Number
PIN - Personal Identification Number (Vehicle Secret Code)
MIN - Model Identification Number

UNIQUE_DOORS_ID :	PS-328001_2
Object Type :	STKH_INFO

Customer Requirement Details

UNIQUE_DOORS_ID :	PS-328001_3
Object Type :	STKH_HEADER

Immobiliser functionality

Requirement - 1:- Immobiliser Authentication
This requirement is about immobiliser security, unauthorised vehicle movement can be prevented by locking the electrical machine, which provides safety and security.
The system comprise of the following units for authentication process:-

1. VCU (Vehicle control unit)
2. IBU (Integrated Body Control Unit)
3. SmartKey FOB (Communicates via LF/RF waves)
4. Start/Stop switch

This requirement is applicable for button driven smart key system which uses encrypted algorithm for secured communication between VCU and IBU through K-Line communication.

Whenever there is request for vehicle start (terminal 15), VCU sends a request signal for IBU to communicate, if there is no response retrial from VCU shall be upto 1.5second.

If positive response from IBU to VCU, auto-detection is processed with smartkey selection and value will be stored in EEPROM memory until the VCU is neutralised.

The IBU unit shall calculate the **'release message communication'** based on the VIN code registered during first key teaching using encryption algorithm ensuring encryption at both the control units.

The transmitted release message serves as an input to VCU, to lock or unlock the electrical machine.

The immobiliser function has two main modes:-

1. **Nominal Mode** - At Ignition ON transition or user attempts to start the vehicle VCU state can switch to released or locked state depend on the authentication result. After receiving the request message from VCU in virgin or neutral or learnt mode and correct MIN mode IMMO ECU will send the response

a) Released state - IMMO_ECU in learnt state (including IMMO ECU VIN code)

b) Lockeded state - no release (without VIN code) (Note:- no check is done with VCU vin code)

After receiving the request message from VCU - virgin or neutral or learnt mode but incorrect MIN code, the IMMO ECU will send the response message as no release anaswer whatever IMMO ECU is in release or lockeded state.

In case of no request message is received from VCU within the timeout TMPVDOUT, immo function should not switch to locked state.

IMMO ECU and VCU communication phase when system working in Nominal mode:-

     a) Ignition On transition phase (**using SMART KEY Fob or backup solution with SMART KEY Fob transponder)**) - When turning On the ignition switch, the IMMO ECU manages a communication window between Immo EcU and VCU with wake-up   signal followed by immo response then release signal or block signal.

     b) Starting phase (**using SMART KEY Fob or backup solution with SMART KEY Fob transponder) -** when user attempts vehicle start in case of VCU Immobilizer state (locked state) the VCU should request to IMMO_ECU for re-authentication.

       It will be able to use the below signal for the Vehicle starting will of the user ;

       After this first « Ignition ON transition » phase or Starting phase a communication between IMMO_ECU& VCU control units takes place.

The VCU control unit controls the E-motor in a normal way for starting and running and starts communication with the IMMO_ECU, sending a VIN request to the IMMO_ECU and waiting for a valid release message from it until the release time period has ended.

In case of IMMO_ECU Immobilizer function state is *« lockeded »*, the IMMO_ECU answer is the « no release » message. VCU enters into the *locked* state, which causes the activation of the immobilization actions of the engine.

In case of IMMO_ECU Immobilizer function state is *« released »*, the IMMO_ECU answer is the « release » message, including the information « IMMO_ECU in learnt mode » and the VIN-code.

If VIN-code received by the VCU is the same as VCU VIN-code, and if MIN-code received by the VCU is the same as VCU MIN-code, VCU enters in the *unlocked* state, which allows to continue the running of the engine.

If VIN-code received by the VCU is different than VCU VIN-code, or if MIN-code received by the VCU is the different than VCU MIN-code, VCU enters in the *locked* state, which causes the activation of the immobilization actions of the engine.

If the EMS doesn't receive a response message from the IMMO_ECU within the release time period, VCU enters in the *locked* state, which causes the activation of the immobilization actions of the engine.

If the IMMO_ECU doesn't send a "*released*" message to the VCU during the defined time-window TMPVDOUT, the IMMO_ECU Immobilizer function swiches in *lockeded* state".

2. **Teaching Mode** - Selected when IMMO ECU receives teaching mode then request from diagnostic tool with correct vehicle secret code PIN code.

MIN code Learning:-
The MIN-code is a fix value, so there is no MIN-code learning procedure.

VCU Neutralisation request:-
For special reason, the Diagnostic tool may ask to IMMO_ECU to send a neutralization request to the VCU in order the VCU changes to the Neutral mode.

The Diagnosis mode VCU neutralization service (from Diagnostic tool to IMMO_ECU) allow getting the "Vehicle Secret Code" (PIN code) corresponding to the vehicle, registered during the Factory mode teaching procedure
Then after, during the release message communication at the next Ignition ON transition, if a correct MIN-code have been received from VCU, the IMMO_ECU(whatever « IMMO in virgin mode » or « IMMO_ECU in neutral mode » or « IMMO_ECU in learnt mode ») will send the response message "VCU should neutralize" instead of other message ("IMMO_ECU in learnt state" or "no release answer" or "IMMO_ECU in Virgin state") with coded VIN Code (this VIN code is data inputed from Diagnostic tool)
(Note : no check is done with the VCU VIN-code)

This response must be sent during all communication phase of the current Ignition ON phase.When Ignition key is cut-off, IMMO_ECU goes back to the nominal mode behavior (no more neutralization request)."

"If there is no Ignition ON transition after neutralization request by Diagnostic tool during 10sec. IMMO_ECU goes back to the nominal mode."

System states:-
1. Virgin state - At the first mounting of the VCU on the car, it is in **Virgin State** and will stay in this mode until it can learn the VIN-code by receiving it from the IMMO_ECU. If no VIN-code is learnt, the VCU stays into this mode, and changes into the *locked* state.
In this mode, the VIN-code stored in VCU non volatile memory is 0FFFFh.
2. Learnt state - When VCU receives the VIN-code and can learn it , it switches to **Learnt State** and changes into the *unlocked* state.
In this mode, VCU checks the IMMO_ECU response at every communication.
3. Neutral state - If the IMMO_ECU response message contains the information « IMMO_ECU in learnt state » and the correct VIN-code and MIN-code, the VCU changes into the *unlocked* state.
If the IMMO_ECU response message contains the information « Neutral mode request » and the correct VIN-code, the VCU switches to the Neutral Mode, set its VIN-code at 0FFFFh value, and changes into the *locked* state.
In the other cases of IMMO_ECU response message (« no release » message, incorrect VIN-code, incorrect MIN-code, ...), the VCU changes into the *locked* state.

For special reason, the IMMO_ECU may ask to the EMS to change to the **Neutral State** , in order to allow the learning of a new VIN-code.

In this mode, if the VCU can learn the VIN-code by receiving it from the IMMO_ECU, the VCU switches to Learning Mode and changes into the *unlocked* state.
If no VIN-code is learnt, the VCU stays into this mode, and into the *locked* state.
In this mode, the VIN-code stored in VCU non volatile memory is 0FFFFh.

VIN code learning:-
Enabling of VIN-code learning is given if VCU VIN-code has the value 0FFFFh. This occurs in the Virgin Mode (after the first mounting of the VCU on the car), and in the Neutral Mode.
In this case, the VIN-code is learnt as soon as response messages are received from IMMO_ECU including the information « IMMO_ECU in learnt state » and the same VIN-codes.

Virgin start for VCU (Twice Ignitiion ON function)

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

The engine can be started by the sequence

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

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

- VCU, smart key system are all Vigin status.
  - 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 number of engine starts by "twice ignition on" is limited. The maximum value is defined by S/W constant. (Value is 32)

Twice ignition ON condition:-
- VCU and smart key system - Virgin only
- 0.5s <= First Ign ON <= 1.5s
- 0.2s <= Ign Off <= 1.5s
- Ignition ON

Twice ignition maximum value = 32 times

Unlocking time of VCU after ign On -30s
The VCU instantly locked by ign off after twice ignition.

Communication services:-

The communication between VCU and ICU is through K-Line serial communication.

VCU is the master and ICU is the slave.

Transmission rate - 4.8kBd +/- 2%

Communication type : Point to point bi-directional transmission between IMMO_ECU and VCU(UART)
Bit format: NRZ

Communication voltage Level:

      Logic "1" :   Transmission Part: More than 80% of battery voltage
                          Reception Part: More than 70% of battery voltage
      Logic "0":   Transmission Part: More than 20% of battery voltage
                          Reception Part: More than 30% of battery voltage

Slope Time: Less than 10% of bit time
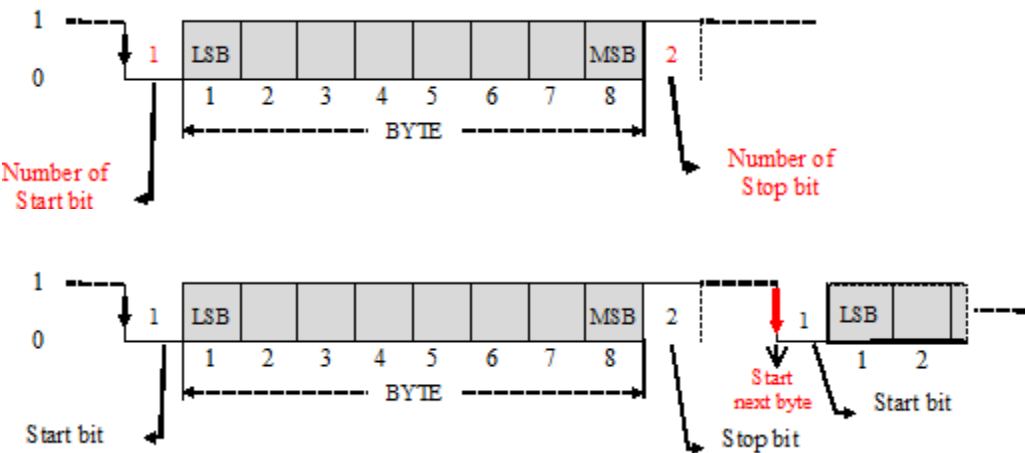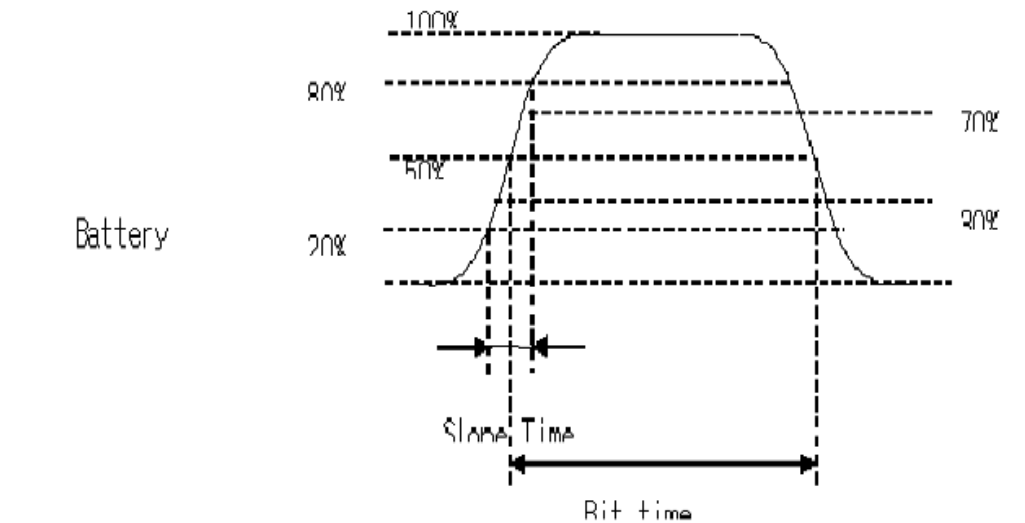
Initialization of communication:-

After Ignition on transition or after user attempts vehicle start in case of VCU **locked** state during Ignition On state, the VCU send the ACK request for immobilizer communication after the initialization time Tini .

The communication frame procedure is followed in order as below (ACK → Authentication)

EMS should not restart the immobilizer communication even if ignition on is issed during the EMS is unlocked

and will send the synchronization if Engine state is changed.

EMS and IMMO_ECU stop the communication if Ign phase is changed from on to off during the immobilizer communication.(EMS don't save the DTC in that case even if No response of IMMO_ECU or DATA Error of IMMO_ECU and IMMO_ECU don't save the DTC in this case even if EMS no request or DATA error of EMS)
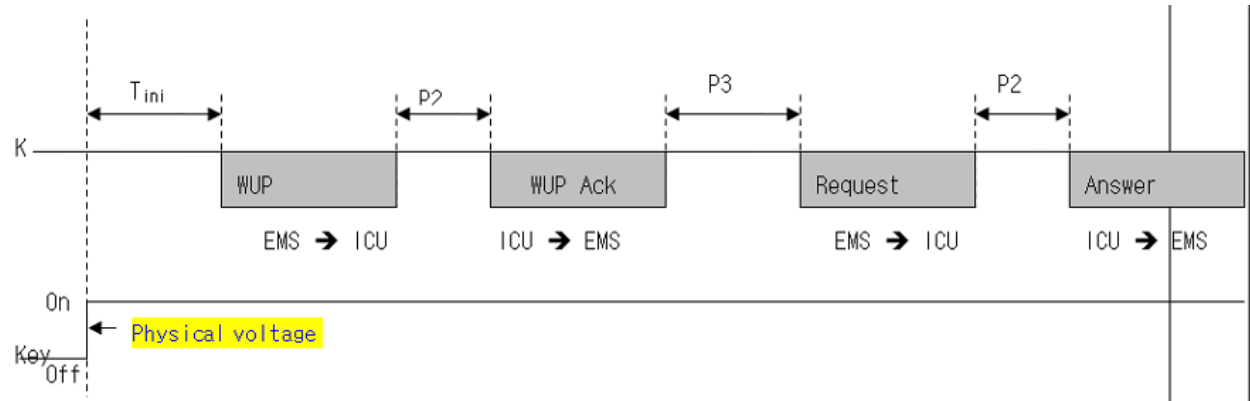
with: 40ms < Tini < 320ms

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

The IGN off filtering Time of EMS/ICU : 1 ms < Tini < 80ms

Remark:

The Tini time will be adjust in order to send the first Wake Up Pattern after the time needed by IMMO_ECU to check the Key (transponder communication time).

P2 : Time between end of VCU Request and start of IMMO_ECU Response
P3 : Time between end of Immobilizer response and start of an VCU new request

Frame structure:-

Page 9 of 19	Created by IBM Rational DOORS 9.7	/VC1CP050/Stakeholder_Requirements/Immo/RQONE03795530_SIA_Base_Software_Suitable_to_Tasking_Compiler
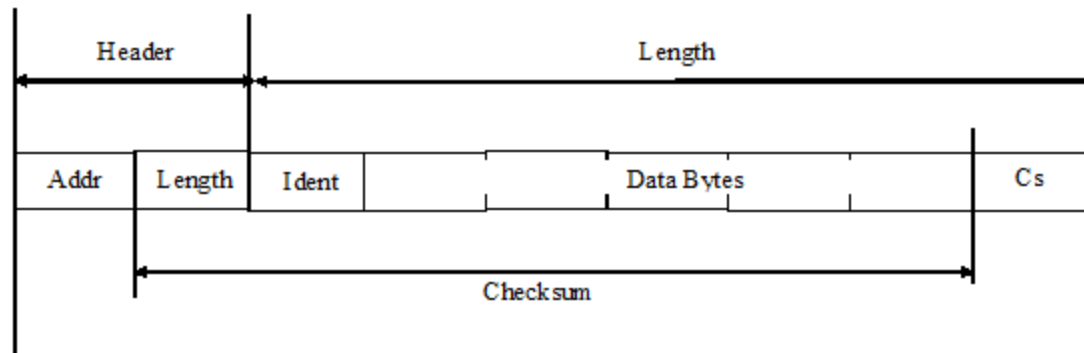
Byte structure:-

Address :-

All messages sent by the VCU will use Address 49H

All messages sent by the IMMO_ECU will use Address 69H

Length :   07H   (always 6 bytes of data and 1 byte for CS)

Data byte:-

Random Number - 2bytes

MIN code - 1byte

VIN Number - 2bytes

Checksum - 1byte

The checksum byte inserted at the end of the message block is defined as the simple 8 bit sum series of all bytes in the message, excluding the Address and the checksum.

NOTE :

1) If the VCU is virgin state or Neutral state , Data Byte 4 and Data Byte 5 are zero.

2) If the IMMO_ECU is virgin state or Neutral state, Data Byte 4 and Data Byte 5 are zero.

Message structure:-

Auto detection:-

VCU Request - 49 02 06 08

Immo ECU Response - 69 02 50 52

The communication is used for setting VCU software to Push start system with VCU state (smartKey1).

If the IMMO_ECU does not respond to this command then it will not be ready to accept other

communications.

VCU has 2 type software(smartKey1 and smartKey2) for Immobilzer and at first Ign On VCU detect which type Immobilizer system is installed and called as VCU autodetection.

VCU Autodetection flow:-
At the first IGN on,

- VCU send the Request signal (49 02 06 08)
- IMMO_ECU send the Response signal(69 02 60 52) : VCU set the software to push start system with VCU state(smartKey1) If VCU received this Response

When VCU detected the Immobilizer type, VCU should keep the software until Neutralization and VCU must not send this request anymore and send the acknowledge signal with VCU state. But IMMO_ECU should send the response (69 02 60 52) anytime regardless of IMMO_ECU type (Virgin, Neutral, Learnt) if VCU send the request for autodetection(49 02 06 08)

Note: VCU should try this communication for 1.5sec If VCU do not receive the response within P2 time.

Wake-up request:-
VCU wake-up request - 49 02 06 08
Immo ECU wake-up response - 69 02 50 52

The communication is used for ancknowledge for communiation of VCU with IMMO_ECU at IGN on.
If the IMMO_ECU does not respond to this command then it will not be ready to accept other communications.
IMMO_ECU will resend the VCU state from VCU.
VCU should try this communication if EMS do not receive the response within P2 time or IMMO_ECU send the different VCU state

Authentication Request:-

VCU Authentication request -

49	**07**	Identifier	RN1	RN2	MIN	VIN1	VIN2	CS

RN1, 2: random number
MIN: 01h (fixed)
VIN1, 2: Coded VIN or Zeros if VCU is virgin or neutral

IMMO ECU Authentication Response

69	07	Identifier	RN3	RN4	MIN	VIN3	VIN4	CS

RN3, 4: coded random number or RN1, 2 from VCU

MIN: 01h (fixed)
VIN3, 4: Coded VIN or Zeros if VCU is virgin or neutral

The communication is used for Immobilizer authentication. VCU can know the IMMO_ECU state and VIN Information. VCU should try the immobilizer communication with the WUP request, If VCU does not receive the response within P2 time or IMMO_ECU send the different VCU state.
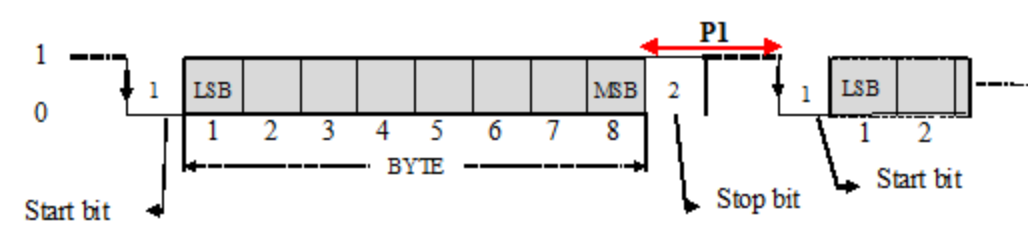
Message Timing:-
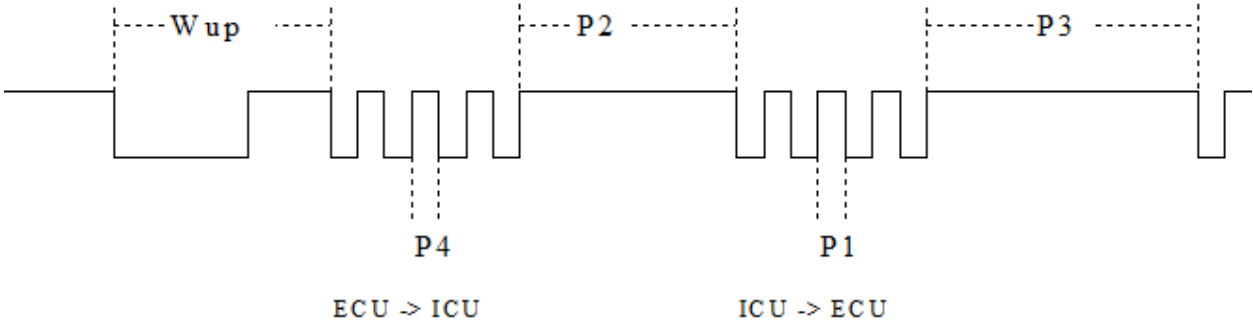
P1 : Inter-byte time for immobilizer request.
P2 : Time between end of VCU request and start of an immobilizer response.
P3 : Time between end of Immobilizer response and start of an VCU new request
P4 : Inter-byte time for VCU request

measurement criteria of P1/P2/P3/P4 timming : include Stop bit (2bit) of before byte / not include Start bit (1bit) of next byte

With :

- Stop bit (2bit) transmission time $\leq P1 \leq$ 1 ms
- 18 ms $\leq P2 \leq$ 40 ms

(the maximum duration for IMMO_ECU to be ready to send the IMMO Status is 400 ms from Key Off->On)

- 1 ms $\leq P3 \leq$ 100ms
- Stop bit (2bit) transmission time $\leq P4 \leq$ 2 ms

After Ignition on transition or
after user attemps engine start in case of VCU *locked* state during Ignition On state,
the VCU ECU starts defined timer (VCU_Communication_Window, tunable parameter, default value 1.5s) for communication between VCU and IMMO_ECU.
In case of no answer message is received from IMMO_ECU within the time-out P2, VCU should be started again communication by sending WUP message until end of timer VCU_Communication_Window.

No Response WUP
EMS should try this communication if VCU do not receive the response within P2 time. This communication will hold on for 1.5sec.
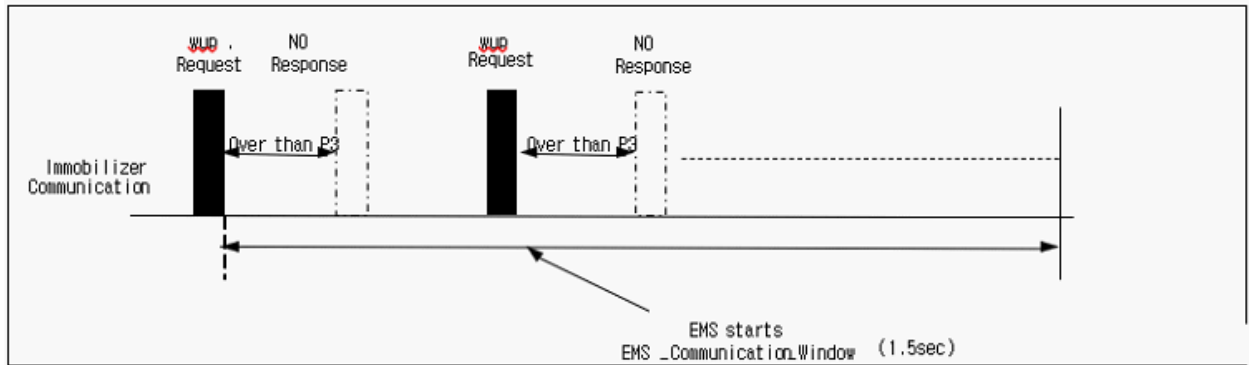
No Response Authentication
EMS should try this communication by sending WUP message if VCU do not receive the

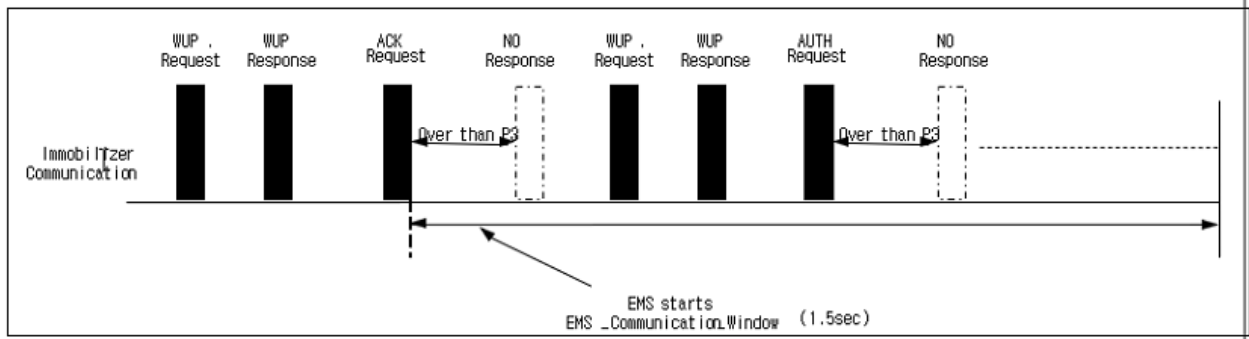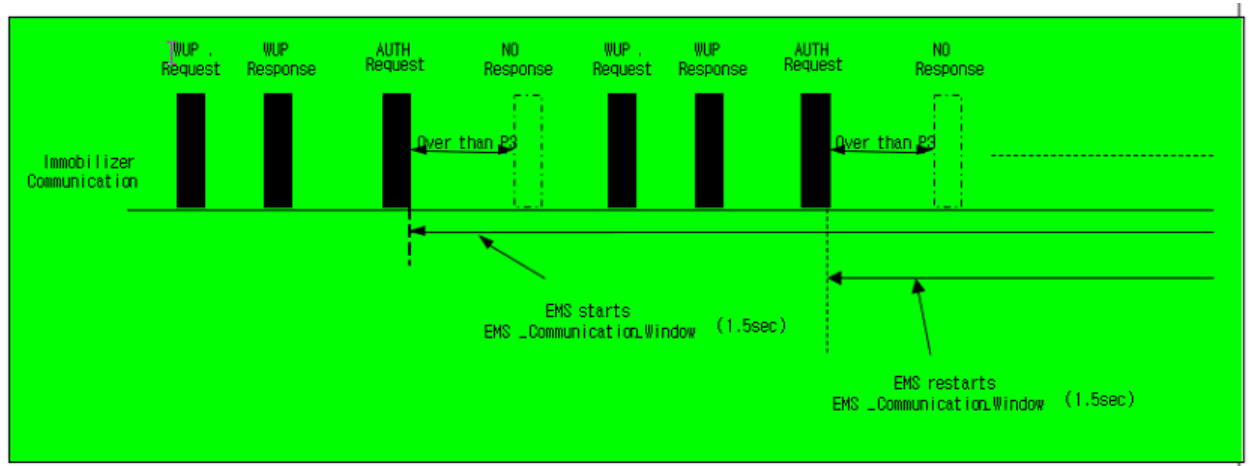| Pa ge 13 of 19	Creat ed by IBM Ratio nal DOO RS 9.7	/VC1CP050/Stakeholder_Requirements/Immo/RQONE03795530_SIA_Base_Softwa re_Suitable_to_Tasking_Compiler

response within P2 time.
This communication will hold on for 1.5sec.

Option-1 :-

Option-2 :-

Communication Error
1)SMARTKEY ECU
During communication with the VCU, 4 kinds of errors are defined:
VCU reception error:
→ No data
→ UART error
→ Frame length error
VCU data error

Page 14 of 19	Created by IBM Rational DOORS 9.7	/VC1CP050/Stakeholder_Requirements/Immo/RQONE03795530_SIA_Base_Software_Suitable_to_Tasking_Compiler

→ Header value
→ Checksum value
→ VCU status Unknown

VCU MIN code error(Wrong MIN code)

These errors set a failure by way of the fault manager for Diagnostic purpose.
"VCU reception error" failure is set after 5 occurrences of error.
"VCU data error" failure, "VCU MIN code error" failure and « No VCU request » failure are set at the first occurrence of error.

Exchange of immobilization status

SERVICES
All messages sent by the VCU will use the Sid= **49h**
All messages sent by the IMMO_ECU will use the Sid= **69h**

MESSAGES
EMS MESSAGES TO IMMO_ECU(Request)

VIN request when VCU is in virgin mode:

Ident	:	03H
RN 1,2	:	random number
MIN	:	01H
VIN1,2	:	Zeros

VIN request when VCU is in neutral mode:

Ident	:	05H
RN1,2	:	random number
MIN	:	01H
VIN1,2	:	Zeros

VIN request when VCU is in learnt mode:

Ident	:	07H
RN1,2	:	random number
MIN	:	01H
VIN1,2	:	Coded VIN

IMMO_ECU MESSAGES TO VCU (Response)

Negative / Neutral mode response for request key Service:

Ident	:	04H (« no release answer »)
RN3,4	:	dummy data (resend RN1,2 received from EMS)

MIN   :   01H

VIN3,4   :   dummy data (resend VIN1,2 received from EMS)

Do not learn key Service:

    Ident   :   09H   (« IMMO_ECU in Virgin state »)

    RN3,4   :   coded random number

    MIN   :   01H

    VIN3,4   :   zeros

Send VIN Service :

    Ident   :   08H   (« IMMO_ECU in Learnt state »)

    RN3,4   :   coded random number

    MIN   :   01H

    VIN3,4   :   coded VIN in IMMO_ECU

Neutralization Service:

    Ident   :   0AH   (VCU should neutralize)

    RN3,4   :   coded random number

    MIN   :   01H

    VIN3,4   :   coded VIN from Diagnostic tool

End of communication:-

The Immobilization communication stops after the release time period (parameter TMPVDOUT) if no Ignition key ON transition occurs. Although Immobilization communication stop, IMMO_ECU should start the communication when VCU request if IGN on.

Immobiliser Status Indicator:-

The status indicator is a LED indicator. It indicates the state of IMMO_ECU immobilizer function and completion of key teaching.

patterns list	LAMP STATE	SYSTEM	
		CAN system	Hard wire system
LAMP_SEQ_ON	LAMP is switched ON	C_ImmoLamp(=0x02)	O_IMMO_IND=ON
LAMP_SEQ_OFF	LAMP is switched OFF	C_ImmoLamp(=0x00)	O_IMMO_IND=Off
LAMP_SEQ_AUTH_ERROR	LAMP is	C_ImmoLamp(=0x01)	O_IMMO_IND=Blinking

	BLINKING 5 times / 1Hz		
Non PIC option	LAMP is switched OFF	C_ImmoLamp(=0x03 or 0x00)	NA

Immo Lamp Blinking
LAMP_Blinking for 10sec when Authentication Fail

    Behavior during learning procedures

While a SmartKey FOB Key learning procedure is in progress, the Lamp is switched OFF.

In addition, LAMP_ON for 700 ms after each successful SmartKey FOB key learnt.

    NeUtral mode
While the IMMO_ECU is in Neutral mode, the Lamp is switched OFF.
In addition, LAMP_SEQ_ON for 700 ms after each successful SMART KEY FOB key learnt.

Requirement - 2:- Re-Authentication by starter key request
After Ignition On, if there is no starter request with valid key more than 30s VCU state shall change from unlocked to locked state and VCU shall start re-authentication at starter key request. Re-authentication procedure is same as authentication procedure at Ignition ON transition.
Requirement - 3:- CIL API
1. uint8 SrvImo_GetImmoReady() - This API shall provide the immobiliser locked or unlocked status based on the authentication result from RB ASW to HMC ASW via the CIL layer.
2. void SrvImo_SetEvReady(void) - This API shall provide EV ready status from RB ASW to HMC ASW via CIL layer.
3. uint8 SrvDfm_GetFltStatus_Immo_P1676(void) - This API shall provide the fault status information when there is data error like header value error or checksum error and timing error when IMMO ECU doesn't respond within P2 time (40ms). Incase VCU receive negative message from Immo ECU fault shouldn't report P1676 fault.
4. uint8 SrvDfm_GetFltStatus_Immo_P1690(void) - This API shall provide fault status information when IMMO ECU does not respond within the P2 (40ms), VCU shall retry the communication again by sending the wake-up request until the end of communication window(1.5s). Incase VCU receive negative message from Immo ECU fault shouldn't report P1690 fault.
5. uint8 SrvDfm_GetFltStatus_Immo_P1696(void) - This API shall provide fault information

when wrong VIN, MIN or Random number is received as response from IMMO ECU and confirmation time shall be 1 time. Incase VCU receive negative message from Immo ECU fault shouldn't report P1696 fault.

6. uint8 SrvDfm_GetFltStatus_Immo_P1699(void) - This API shall provide fault information when twice ignition counter exceeded 32 or more times.

7. uint8 SrvImo_GetCommStatus(void) - This API shall provide the immobiliser communication status with VCU unit.

Refer below communication status information:-

0: CPXIMO_KCOMSTATE_UNINIT
1: CPXIMO_KCOMSTATE_INIT
2: CPXIMO_KCOMSTATE_REQ_AUTODETECTION
3: PXIMO_KCOMSTATE_RESP_AUTODETECTION
4: CPXIMO_KCOMSTATE_REQ_WAKEUP
5: CPXIMO_KCOMSTATE_RESP_WAKEUP
6: CPXIMO_KCOMSTATE_REQ_ACK
7: CPXIMO_KCOMSTATE_RESP_ACK
8: CPXIMO_KCOMSTATE_REQ_AUTEN
9: CPXIMO_KCOMSTATE_RESP_AUTHEN
10: CPXIMO_KCOMSTATE_PENDING_AUTHEN
11: CPXIMO_KCOMSTATE_NOT_RESP
12: CPXIMO_KCOMSTATE_NOT_MATCH_RESP
13: CPXIMO_KCOMSTATE_NOT_MATCH_AUTHEN
14: CPXIMO_KCOMSTATE_TIMEOUT_WINDOW
15: CPXIMO_KCOMSTATE_FINISH_COMM
16: CPXIMO_KCOMSTATE_TWICE_IGN
17: CPXIMO_KCOMSTATE_LEARNT_VIN
18: CPXIMO_KCOMSTATE_SHOULD_NEUTRALIZE
19: CPXIMO_KCOMSTATE_UNLOCKING
20: CPXIMO_KCOMSTATE_CRANKING_TIMEOUT
21: CPXIMO_KCOMSTATE_TWICE_TIMEOUT
22: CPXIMO_KCOMSTATE_NOT_RESP_SEND
23: CPXIMO_KCOMSTATE_NOT_RESP_WAIT
24: CPXIMO_KCOMSTATE_REQ_SEND_WAIT
25: CPXIMO_KCOMSTATE_NOT_MATCH_RESP_WAIT
26: CPXIMO_KCOMSTATE_NOT_MATCH_RESP_SEND
27: CPXIMO_KCOMSTATE_REQ_SYNC
28: CPXIMO_KCOMSTATE_RESP_SYNC
0xFF: CPXIMO_KCOMSTATE_UNDEFINED

8. void SrvImo_SetVirginImmo(bool RetVal) - This API shall change the learnt VCU state to virgin.

Requirement - 4:-Random number generation by HSM

Background:-

Earlier developed software random number was generated by an internal API, during workshop with HMC a new request was made to implement the s/w were random number shall be generated from HSM.

Solution:-

Random number shall be generated using the HSM API with unique random number value for each authentication request.

Refer. shared by customer - ES95489-21 for random number generation from HSM.

UNIQUE_DOORS_ID :	PS-328001_4
Object Type :	STKH_FUNC_REQ
Internal Comment :	Microsoft Word Document
Allocation :	[SYSTEM]
Affected Component :	SF_Imob and SF component for **SwShHMC** has been requested to prj. once component details received will be updated.
Safety Classification :	QM
CRQ :	RQONE04354630
Status :	READY_FOR_INTERNAL_REVIEW
RT-ID :	RTBBM930372 is pending for the '_Status_' attribute. Review link -> https://rb-bbm-reviewtool01.apps.intranet.bosch.com/ReviewTool/?BU=ALM&RID=RTBBM930372