CAN Network Management Requirement Specification

(Base on AUTOSAR NM)

Version 1.5

<Confidential>

Geely Automobile Research Institute

Revision history

Version	**Version Description** (Draft/Modification /Released)	**Compiled by** Department Name **Date**	**Review by** Department Name **Date**	**Approval by** Department Name **Date**	**Description**
V0.1	Draft	EE Division IVN Department; Liu Tong 2014-06-23	EE Division IVN Department; Cai Weijie 2014-07-22	Department Name Date	
V0.2	Modification	EE Division IVN Department; Cai Weijie 2014-08-19	EE Division IVN Department; Li Liangxu 2014-08-19	Department Name Date	
V1.0	Released	EE Division IVN Department; Cai Weijie 2014-08-27	EE Division IVN Department; Li Liangxu 2014-08-27	EE Division IVN Department; Wang Juan 2014-08-27	
V1.0	Released	EE Division IVN Department; Cai Weijie Liu Tong 2014-10-07	EE Division IVN Department; Li Liangxu 2014-10-07	EE Division IVN Department; Wang Juan 2014-10-07	Update according to KC/FE project's feedback
V1.1	Released	EE Division IVN Department; Cai Weijie 2015-04-20	EE Division IVN Department; Li Liangxu 2015-04-23	EE Division IVN Department; Fu ZhaoHui 2015-04-27	
V1.2	Released	EE Division IVN Department; Cai Weijie 2015-06-11	EE Division IVN Department; Li Liangxu 2015-06-12	EE Division IVN Department; Fu ZhaoHui 2015-06-15	
V1.3	Released	EE Division IVN Department; Cai Weijie 2016-05-05	EE Division IVN Department; Li Liangxu 2016-05-06	EE Division IVN Department; Fu ZhaoHui 2016-05-09	
V1.4	Draft	GRI EE Department; Zhu Zhenglong 2016-07-22	GRI EE Department; Zhu Zhenglong 2016-07-22	GRI EE Department; Zhu Zhenglong 2016-07-22	
V1.5	Released	GRI EE Department; Zhu Zhenglong 2017-11-13	GRI EE Department; Zhu Zhenglong 2017-11-13	GRI EE Department; Zhu Zhenglong 2017-11-13	

Change log

Table 1 Change history

Version	Section	Detailed description of change
V0.1	ALL	First Version;
V0.2	3.2.1	Delete the decription of Lost Communication detection and healing Strategy
V0.2	3.2.1	Define $T_{DiagEnable}$ in table 12.
V1.0	3.2.2	Add condition 'Ignition state shall be IGN ON' for lost communication self-diagnosis
	3.1	Redefine Default Value and Substitute Value
V1.1	1.4	Add the References Specification [4] and [5]
	2.3	Add the condition that set the Active Wake up bit zero.
	2.3	Add the definition of user data 2-5.
	3.2.1	Update the conditon of Lost communicatioin detection.
	2.4	Change the NM node address ranges from 0x00-0xFF to 0x00-0x7F.
	2.4	Delete the ECU NM ID table. Note: the NM ID is defined in Geely ECU Address Specification.
	2.2.3.3.1/ 2.5	Update the definition of T_START_NM_TX
	2.2.3	Prohibit the TX and Rx of App msg in Prepare Bus Sleep Mode but the The Frame already in Tx Buffer is allowed to send.
	2.2.3	Add the note:" After power on, the ECU shall stay in Bus Sleep Mode until the condition 1 or condition 2 meet."
	3.3.2	Add the description: "begins with Repeat Message State and does not use the Immediate Transmission Mechanism."
	1.3	Add the Abbreviations of Power on.
	2.3	Add the description of Repeat Message Request Bit, Active Wakeup Bit and network management state Bit.
V1.2	3.3.2	Delete the description:" begins with Repeat Message State and does not use the Immediate Transmission Mechanism."
	3.3.3	Delete the description: "the condition of TDiagEnable is met".
V1.3	2.9	Add the definition of ECU startup.
	3.2.2	Update the enable condition of Lost Communication Self-Diagnosis.
	3.3.2	Update the definition of CAN BUS-OFF Handling and Recovery.
	2.4	Add the description: "monitor the all NM message IDs within this range".
	2.4	Delete the discription: "NM ECU Address of Geely CAN has been defined in Geely ECU Address Specification."
	1.4	Delelte the References Specification [5].
V1.4	2.7.1	Add definition on ECU in diagnostic session
	4	Add definition of communication diagnostic voltage

Version	Section	Detailed description of change
V1.5	1.4	Update "[3] Geely Diagnostic Requirement Specification" to "[3] Geely DTC List";
	2.2.3.3.2	Update the description of entering the Repeat Message State because Repeat Message Request Bit is one;
	2.2.3.3.3	Update the description of entering the Repeat Message State because Repeat Message Request Bit is one;
	2.2.4	Update the Condition 7 from "Repeat Message Bit Received" to "Repeat Message Request Bit Received". Update the Condition 9 to Reserved.
	2.3	Add the description: "When entering Repeat Message State from Normal Operation State and Ready Sleep State because of received Repeat Message Request Bit (Condition 7) is set to one, the receiving ECU's Repeat Message Request Bit shall be keep zero".
	2.9	Update the description to ①: local conditions active or received NM PDU
	3.1	Delete "This kind of substitute value is specified for each signal in CMX [2]."
	3.2.3	Add definition of CAN Communication error Diagnosis.
	3.3.3	Update the definition of CAN BUS-OFF Self-Diagnosis;
	3.4	Update the definition of Under/Over Voltage Strategy

Table of Contents

1 General

This document – Network Management Requirement Specification (NMRS) - specifies the requirements for a specific network management software component and the methods to be used to ensure that each requirement has been met.

Requirements defined hereafter are common to **KL30 ECUs** connecting to the CAN communication system.
Exceptions to this specification shall be explicitly noted and approved by Geely officially.

1.1 Scope

The document covers the requirements for Network management and network related diagnostic and network behavior.

In this document, the following defined terminology prescription applies. The usage of

– “Shall” expresses in the text a mandatory requirement.

– “Should” expresses in the text an optional requirement.

– “Can” expresses in the text a permitted practice or method.

1.2 General Design Requirements

The CAN architecture sees Figure 1.

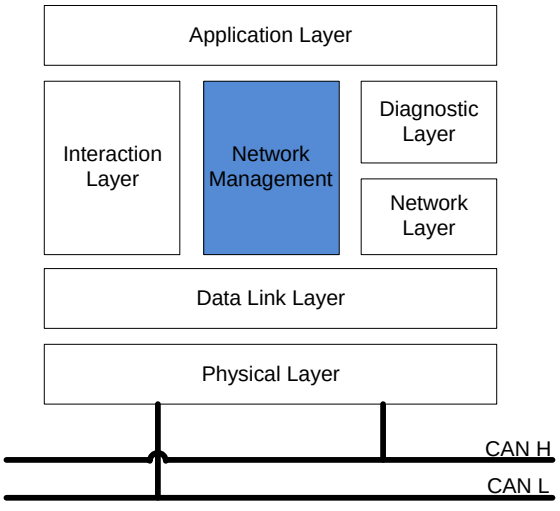

Figure 1 CAN Architecture

The CAN Network Management is a hardware independent protocol that can only be used on CAN. Its main purpose is to coordinate the transition between normal operation and bus-sleep mode of the network and error handling for a node.

The network management layer is specified in details in the following chapter, which is based on the AUTOSAR NM state chart.

1.3 Abbreviations, Acronyms, Definitions & Symbols

Definition	Description
Clamp 15 or KL 15	A power supply/control signal that activate nodes
Clamp 30 or KL 30	A permanent power supply
ECU	An electronic control unit that execute software
Power On	The KL 30 is re-connected.
Node	Same as node in this document, see ECU

Abbr.	Stand for
DTC	Diagnostic Trouble Code
NM	Network Management
CMX	CAN Matrix

1.4 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] Geely CAN Communication Requirement Specification

[2] Geely In Vehicle CAN Communication Matrix

[3] Geely DTC List

[4] 4.1.3 AUTOSAR_SWS_CAN Network Management 3.6.0

2 Network Management

2.1 Network management overview

This chapter defines the Network Management requirements for KL 30 Nodes.

KL30 nodes will still require CAN bus communication after ignition switched OFF.

KL30 Node implements a same NM protocol for a control units connected through a CAN network.

2.2 Network management function

2.2.1 NM Functional Algorithm

The Geely NM is based on decentralized direct network management strategy, which means that every network node performs activities self-sufficient depending on the NM PDUs only that are received or transmitted within the communication system.

The NM algorithm is based on periodic NM PDUs, which are received by all nodes in the cluster via broadcast transmission. Reception of NM PDUs, indicates that sending nodes want to keep the network management cluster awake. If any node is ready to go to the Bus Sleep Mode, it stops sending NM PDUs, but as long as NM PDUs from other nodes are received, it postpones transition to the Bus Sleep Mode. Finally, if a dedicated timer elapses because no NM PDUs are received anymore, every node initiates transition to the Bus Sleep Mode.

If any node in the network management cluster requires bus communication, it can wake up the network management cluster from the Bus Sleep Mode by transmitting NM PDUs.

The main concept of the Geely NM algorithm can be defined by the following two key-requirements:

- Every network node in a NM cluster shall transmit periodic NM PDUs as long as it requires bus-communication; otherwise it shall transmit no NM PDUs.
- If bus communication in a NM cluster is released and there are no NM PDUs on the bus for a amount of time determined by T_NM_TIMEROUT + T_WAIT_BUS_SLEEP transition into the Bus Sleep Mode shall be performed.

2.2.2 NM Transition Diagram

The network management state chart diagram was defined in this section. Refer to Figure 2.

2.2.3 NM Mode Description

The Geely network management shall contain three modes:

- Bus Sleep Mode
- Prepare Bus Sleep Mode
- Network Mode

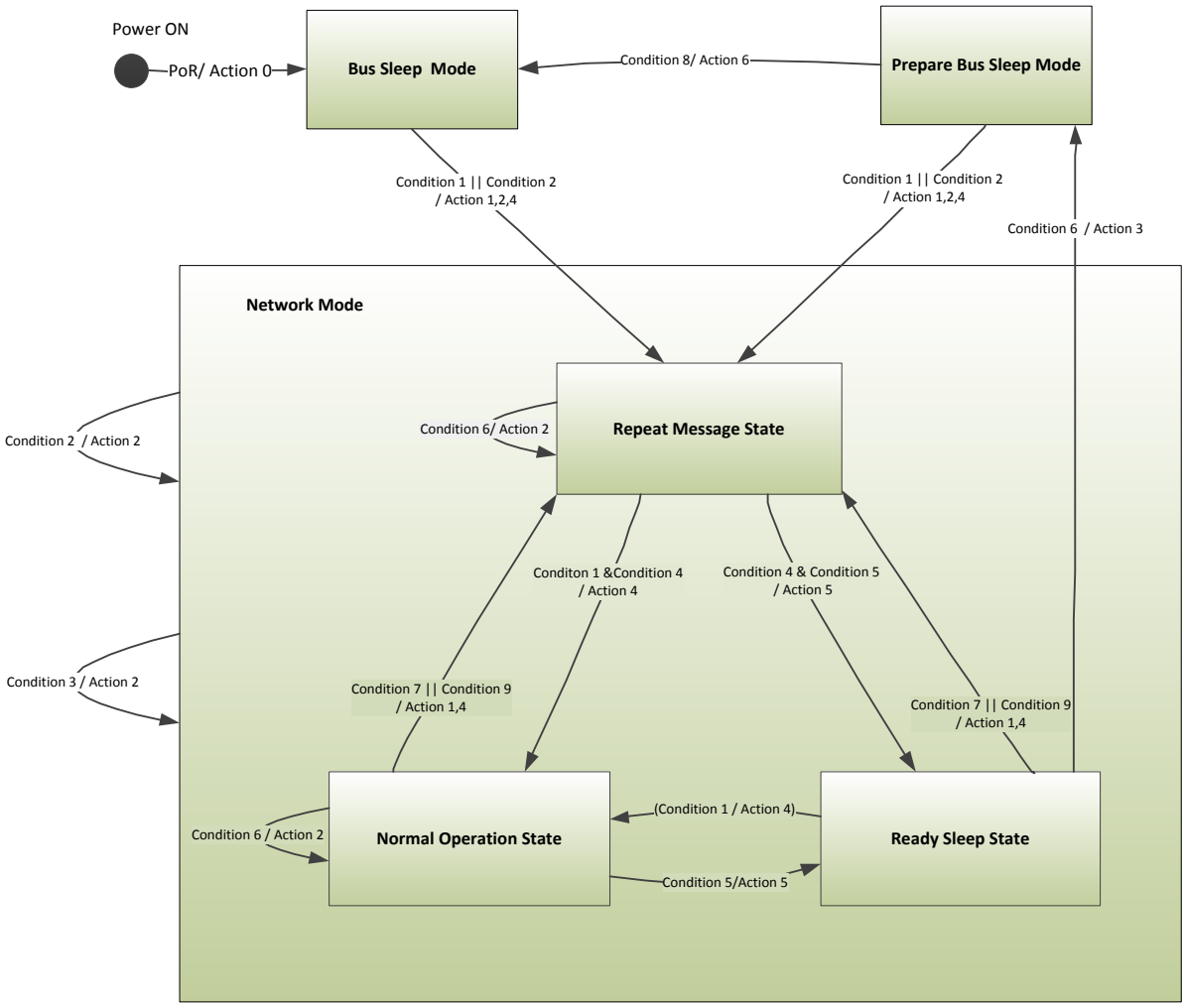

Figure 2 Geely NM Transition Diagram

Note: After power on, the ECU shall stay in Bus Sleep Mode until the condition 1 or condition 2 meet.

The table 2 describes to send different type of message in different mode of network:

Table 2 different type of message in modes of network

NM Mode		NM Frame		App Frame[1]	
		Tx	Rx	Tx	Rx
Bus Sleep Mode		N	Y	N	N
Prepare Bus Sleep Mode		N	Y	N[2]	N
Network Mode	Repeat Message State	Y	Y	Y	Y
	Normal Operation State	Y	Y	Y	Y
	Ready Sleep State	N	Y	Y	Y

'N' denote that frame of Tx/Rx is impossible.
'Y' denote that frame of Tx/Rx is possible.
[1] App frames include application messages, diagnosis messages, calibration messages;
[2] The Frame already in Tx Buffer is allowed to be send.

2.2.3.1 Bus Sleep Mode

The purpose of the Bus Sleep Mode is to reduce power consumption in the node when no messages are to be exchanged. The communication controller is switched into the sleep mode, respective wakeup mechanisms are activated and finally power consumption is reduced to the adequate level in the Bus Sleep Mode.

2.2.3.2 Prepare Bus Sleep Mode

The purpose of the Prepare Bus Sleep Mode is to ensure that all nodes have time to stop their network activity before the Bus Sleep Mode is entered. In Prepare Bus Sleep Mode the bus activity is calmed down (i.e. queued messages are transmitted in order to make all Tx-buffers empty) and finally there is no activity on the bus in the Prepare Bus-Sleep Mode.

When the NM module is entered in the Prepare Bus Sleep Mode and start immediately T_WAIT_BUS_SLEEP timer, after that time the Prepare Bus Sleep Mode shall be left and the Bus Sleep Mode shall be entered.

At successful reception of a NM PDU in the Prepare Bus Sleep Mode, the NM Module shall enter the Network Mode; by default the NM Module shall enter the Repeat Message State.

When the network is requested in the Prepare Bus Sleep Mode, the NM module shall immediately enter the Network Mode; by default the NM Module shall enter the Repeat Message State.

2.2.3.3 Network Mode

The Network Mode shall consist of three internal states:

- Repeat Message State
- Normal Operation State
- Ready Sleep State

When the Network Mode is entered from Bus Sleep Mode, by default, the NM module shall enter the Repeat Message State.

When the Network Mode is entered from Prepare Bus Sleep Mode, by default, the NM module shall enter the Repeat Message State.

When the Network Mode is entered, the NM module shall start the T_NM_TIMEROUT Timer.

At successful reception of a NM PDU in the Network Mode, the NM module shall restart the T_NM_TIMEROUT Timer.

At successful transmission of a NM PDU in the Network Mode, the NM module shall restart the T_NM_TIMEROUT Timer.

The NM module shall reset the T_NM_TIMEROUT Timer every time it is started or restarted.

- Wake Up Time Definition

When the sleeping ECU was waked up by local conditions or received NM PDU, ECU will enter Network Mode, by default the NM Module shall enter the Repeat Message State, and start sending the first NM PDU. This process should be complete within specified time that is denoted by ‘t , where t<=T_WakeUp.

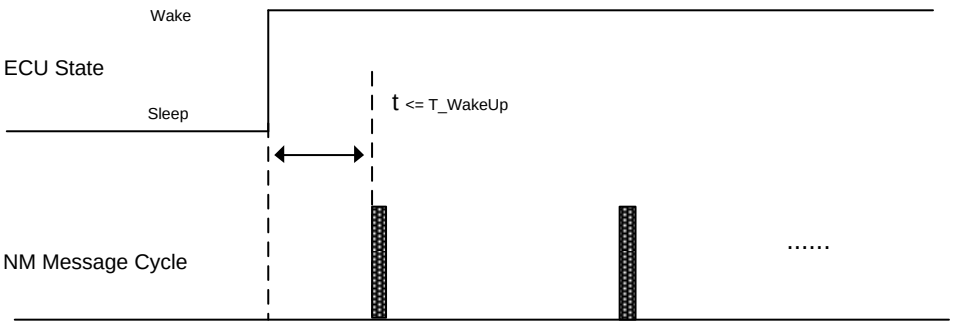

Figure 3 Wake Up time definition

2.2.3.3.1 Repeat Message State

The Repeat Message State ensures that any transition from Bus Sleep Mode or Prepare Bus Sleep to the Network Mode becomes visible to the other nodes on the network. Additionally it ensures that any node stays active for a minimum amount of time. It can be used for detection of present nodes.

When the Repeat Message State is entered from Bus Sleep Mode, Prepare Bus Sleep Mode, Normal Operation State or Ready Sleep State, the NM module shall (re-)start transmission of NM PDUs.

When the T_NM_TIMEROUT Timer expires in the Repeat Message State, the NM module shall start the T_NM_TIMEROUT Timer.

The network management state machine shall stay in the Repeat Message State for the amount of time determined by the T_REPEAT_MESSAGE; after that time the NM module shall leave the Repeat Message State.

When Repeat Message State is left and if the network has been requested, the NM module shall enter the Normal Operation State.

When Repeat Message State is left and if the network has been released, the NM module shall enter the Ready Sleep State.

When Repeat Message State is left, the NM module shall clear the Repeat Message Bit.

- Immediate Transmission Mechanism

The immediate transmission mechanism is used for nodes which want to immediately wake up the bus or restore communication as fast as possible.

If the Repeat Message State is entered via Network Request (local conditions) or Repeat Message Request, the required number of immediate NM PDUs transmissions shall be started immediately, this can be illustrated by Figure 4.In other cases, entering the repeat message state caused by successfully received NM PDUs or received the Repeat Message Request Bit Indication, the NM message shall be sent by T_NM_MessageCycle after entering the Repeat Message State, this can be illustrated by Figure 5.

When entering the Repeat Message State from Bus Sleep State or Prepare Bus Sleep State because of Network Request, the NM PDUs shall be transmitted using T_NM_ImmediateCycleTime as cycle time. The transmission of the first NM PDU shall be triggered as soon as possible. After the transmission the Message Cycle Timer shall be reloaded with T_NM_ImmediateCycleTime. The T_NM_MessageCycle shall not be applied in this case.

When entering the Repeat Message State from Normal Operation State or Ready Sleep State because of Repeat Message Request, the NM PDUs shall be transmitted using T_NM_ImmediateCycleTime as cycle time. The transmission of the first NM PDU shall be triggered as soon as possible. After the transmission the Message Cycle Timer shall be reloaded with T_NM_ImmediateCycleTime. The T_NM_MessageCycle shall not be applied in this case.

The number of NM PDUs transmitted with the cycle time T_NM_ImmediateCycleTime is defined N_ImmediateNM_TIMES. After all immediate NM PDUs have been transmitted the NM shall start transmission using the cycle time T_NM_MessageCycle.

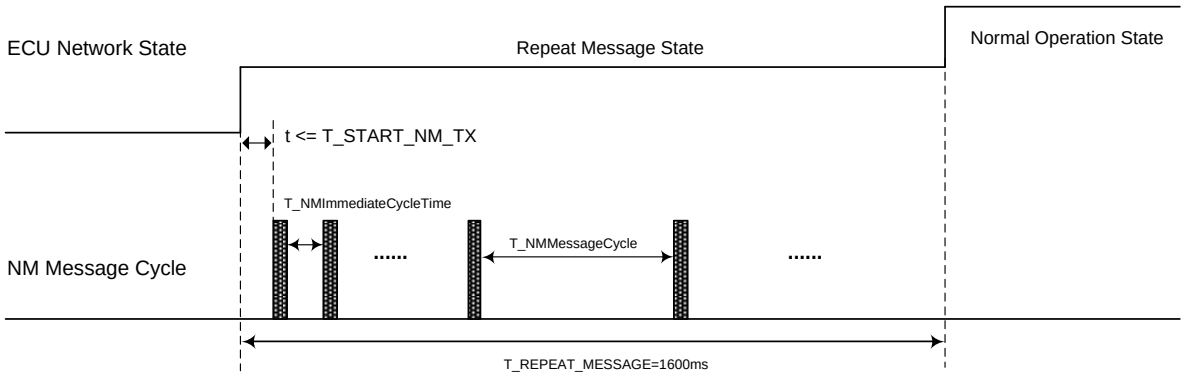

Figure 4 NM immediate message cycle definitions

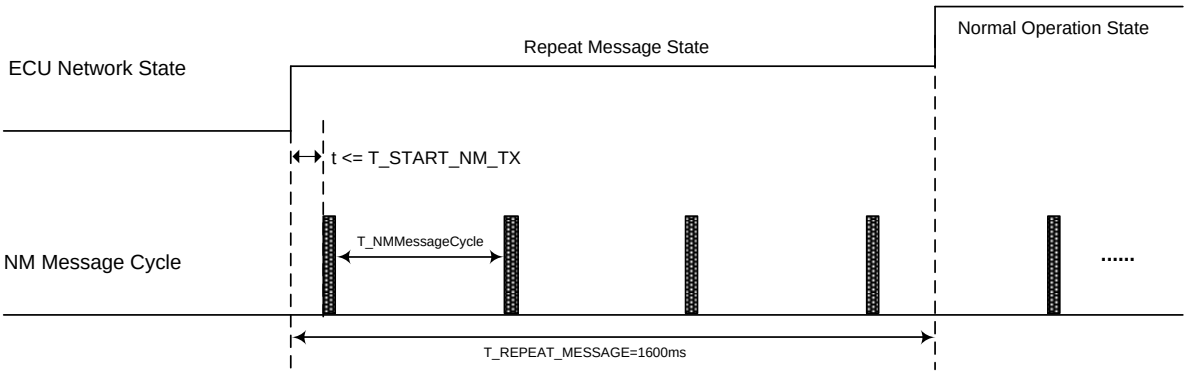

Figure 5 NM message cycle definition

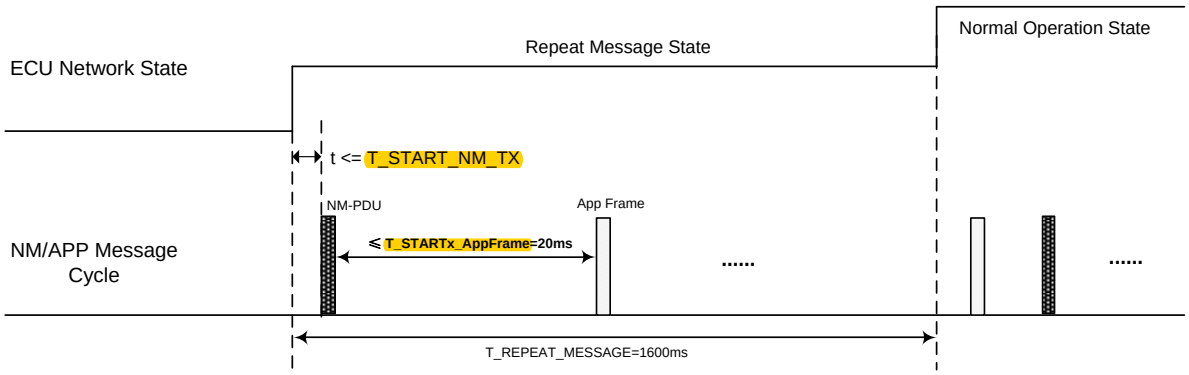

Figure 6 T_STARTx_AppFrame definition

- Start NM Time Definition

When the Repeat Message State is entered from Prepare Bus Sleep Mode, Normal Operation State or Ready Sleep State, the first NM PDUs should be transmitted within 't', where the t<=T_START_NM_TX.
T_REPEAT_MESSAGE is a minimum amount of time during which other nodes on CAN bus can be waked up by receiving NM frame. After this timer elapses, node will transit to Normal Operation State or Ready Sleep State.
CAN application frame should be sent within the T_STARTx_AppFrame in this state after the first NM frame was successfully sent. It can be illustrated by Figure 6.

2.2.3.3.2 Normal Operation State

The Normal Operation State ensures that any node can keep the network management cluster awake as long as the network is requested.
When the Normal Operation State is entered from Repeat Message State or Ready Sleep State, the NM module shall start transmission of NM PDUs with T_NM_MessageCycle Period.
When the T_NM_TIMEROUT Timer expires in the Normal Operation State, the NM module shall start the T_NM_TIMEROUT Timer.
When the network is released and the current state is Normal Operation State, the NM module shall enter the Ready Sleep State.
When receiver received Repeat Message Request Bit is one, the NM module shall enter the Repeat Message State.
At Repeat Message Request in the Normal Operation State, the NM module shall enter the Repeat Message State, the NM module shall set the Repeat Message Bit and start the immediate mechanism.

2.2.3.3.3 Ready Sleep State

The Ready Sleep State ensures that any node in the network management cluster waits with transition to the Prepare Bus Sleep Mode as long as any other node keeps the network management cluster awake.
When the Ready Sleep State is entered from Repeat Message State or Normal Operation State, the NM module shall stop transmission of NM PDUs.
When the T_NM_TIMEROUT Timer expires in the Ready Sleep State, the NM module shall enter the Prepare Bus Sleep Mode.
When the network is requested and the current state is the Ready Sleep State, the NM module shall enter Normal Operation State.
When receiver received Repeat Message Request Bit is one, the NM module shall enter the Repeat Message State.
At Repeat Message Request in the Ready Sleep State, the NM module shall enter the Repeat Message State. the NM module shall set the Repeat Message Bit and start the immediate mechanism.

2.2.4 NM State Transitions

NM State Transition Conditions:

Table 3 NM Transition Conditions

Condition No.	Description
Condition 1	Network Requested (local condition)
Condition 2	Successfully Received NM PDU.
Condition 3	Successfully Transmit NM PDU.
Condition 4	T_REPEAT_MESSAGE timer has expired.
Condition 5	Network Released.(e.g. local node sleep condition is true)
Condition 6	T_NM_TIMEROUT has expired.
Condition 7	Repeat Message Request Bit Received.
Condition 8	T_WAIT_BUS_SLEEP timer has expired.
Condition 9	NM Repeat Message Request. (e.g. Master node request)

NM State Transition Actions:

Table 4 NM Transition Actions

Action No.	Description
Action 0	Initialization Of NM
Action 1	Start T_REPEAT_MESSAGE Timer.
Action 2	Start T_NM_TIMEROUT Timer.
Action 3	Start T_WAIT_BUS_SLEEP Timer.
Action 4	Node Transmitting NM PDU.
Action 5	Stop Transmit NM PDU
Action 6	Go to Sleep Mode

2.3 NM Control Frame Data Format

The table 5 below shows the default format of the NM frame:

Table 5 NM Control Frame Data Format

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte 0	ECU Address							
Byte 1	Control Bit Vector							
Byte 2	User data 0							
Byte 3	User data 1							
Byte 4	User data 2							
Byte 5	User data 3							
Byte 6	User data 4							
Byte 7	User data 5							

The user data 0 is used to wake up reason, i.e. the network request conditions, that are defined in ECU specification as well as CMX.

The first bit in user data 1 is used to indicate network management state (whether running in Repeat Message Mode or not), which is defined in CMX. It's only used for test.

The user data 2-5 are used to keeping CAN bus awake reasons that are defined in ECU specification as well as CMX. The ECU shall transmit all current application reasons, which prevent the ECU to Ready Sleep State.

The table 6 below describes the format of the Control Bit Vector:

Table 6 The Format of the Control Bit Vector

Byte 1	Control Bit Vector	Interpretation
bit 0	Repeat Message Request	0: Repeat Message State not requested 1: Repeat Message State requested
bit 1	Res	
bit 2	Res	
bit 3	Res	
bit 4	Active Wakeup Bit	0: Node has not woken up the network (passive wakeup) 1: Node has woken up the network (active Wakeup)
bit 5	Res	
bit 6	Res	
bit 7	Res	

The Default value of Repeat Message Request is zero. When entering Repeat Message State from Normal Operation State and Ready Sleep State because of Repeat Message Request (Condition 9), the Repeat Message Request Bit is set to one until re-enter the Normal Operation State and Ready Sleep State.

When entering Repeat Message State from Normal Operation State or Ready Sleep State because of received Repeat Message Request Bit (Condition 7) is set to one, the receiving ECU's Repeat Message Request Bit shall be keep zero.

When entering the Repeat Message State from Bus Sleep State or Prepare Bus Sleep State because of Network Request (local wake up conditions), the NM module should be set Active Wakeup Bit to value of one until re-enter the Prepare Bus Sleep State.

When entering the Repeat Message State because of remote wake up message, the NM module should be set Active Wakeup Bit to value of zero.

2.4 NM Control Frame Identifier

CAN Identifier range from 0x400 ~ 0x47F, are used for ECU network management control frames as shown in Table 7.

Table 7 NM Control Frame CAN ID Design

Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
NM Control Frame Base Address			ECU Address							

Formula: NM Message ID = NM Control Frame Base Address + ECU Address.

All participants of network management ECU shall follow this formula to monitor the all NM message IDs within this range, and do the right actions, in order to develop a network management platform of Geely.

NM Control Frame base address:

Table 8 NM Control Frame Base Address

NM Control Frame Base Address	Description
0x400	NM CAN ID started from this address

2.5 NM Timing Control Parameter

NM time control parameters are defined as in Table 9.

Table 9 CAN NM Control Timing Design

Timer name	Value	Tolerance	Description
T_REPEAT_MESSAGE	1600ms	+/-10%	Timer for a node becomes visible to the other nodes on the network.
T_NM_TIMEOUT	2000ms	+/-10%	As long as the node enter the network mode and start this timer. When the timer is expired, the node will enter the Prepare Bus Sleep Mode.
T_WAIT_BUS_SLEEP	2000ms	+/-10%	The timer is to ensure that all nodes have time to stop their network activity.
T_START_NM_TX	10ms	+/-10%	The time describes all sent NM message behaviour that the NM node enters network mode from Prepare Bus Sleep Mode, Normal Operation State or Ready Sleep State and start to transmit the first NM PDU. This time may be zero millisecond, one millisecond, two milliseconds and so on, but ten milliseconds is maximum time.
T_STARTx_AppFrame	20ms	+/-10%	The maximum interval time starts sending application message after send the first NM-PDU successfully.
T_NM_ImmediateCycleTime	20ms	+/-10%	In generally, network request of node should be trigger the immediate transmission mechanism and NM-PDU will be transmitted with this periodic in Repeat Message State.
T_NM_MessageCycle	500ms	+/-10%	The interval time is every two NM frames which are transmitted in Network Mode except Ready Sleep State.
T_WakeUp	100ms	+/-10%	The value is max time that the node from the Sleep Mode to Network Mode and send the first NM PDU, generally transmit in Repeat Message State.
N_ImmediateNM_TIMES	5		The number of NM PDUs transmitted with the cycle time T_NM_ImmediateCycleTime in Repeat Message Mode.

2.6 Network Request Condition

The specific request conditions of ECUs shall be discussed with supplier and defined in ECU specification during the process of development of network functions.

2.7 Network Release Condition

The specific release conditions of ECUs shall be discussed with supplier and defined in ECU specification during the process of development of network functions.

2.7.1 ECU in diagnostic session

Generally, ECU node must not be waked up by diagnostic messages when in sleep mode (NM at Bus Sleep Mode, or Prepare Bus Sleep Mode), also node must not go to sleep mode when it's in diagnostic session (NM at Network Mode).

Diagnostic software module inform NM its communication requirement by interfaces of Network Request and Network Release.

There are some typical cases listed below:

- When receive diagnostic message in Ready Sleep State, diagnostic software module must send Network Request to NM to transfer to Normal Operation State, in diagnostic application, it will start a $T_{Wait\_DiagReq}$ timer. Diagnostic application shall send Network Release to NM to tell NM return back to Ready Sleep State when $T_{Wait\_DiagReq}$ timer is expired (other applications still need network communication, Network Release command should be negotiated by all applications to send out).

Table 10: Time Parameter of $T_{Wait\_DiagReq}$

Time	Typical（S）	Tolerance
$T_{Wait\_DiagReq}$	5	±10%

Note： $T_{Wait\_DiagReq}$ *is a timer that keep the node wake up reason after received the diagnostic request message . The* $T_{Wait\_DiagReq}$ *timer shall restart after received a diagnostic request message.*

- The node must not transfer to Network Mode when received diagnostic message in Bus Sleep Mode or Prepare Bus-Sleep Mode. If ECU have special function requirement, it shall be permitted by Geely.

The following figures give a sample on handling of the network management state machine when received the diagnostic message (supposed only diagnostic application needs network communication).

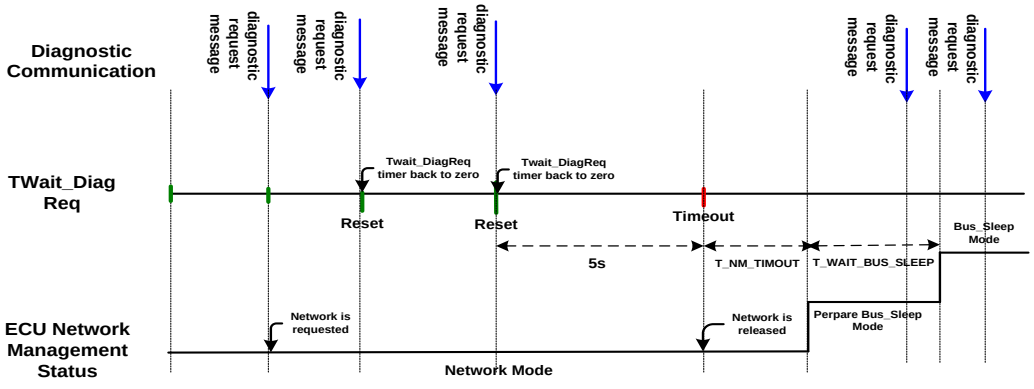

Figure 7 Network management state machine transference with diagnostic communication

More details on diagnostic, please refer to Geely diagnostic specification.

2.8 NM OF Fault Operation

NM on a node which is or become bus unavailable shall have a deterministic behaviour. NM on a node which is or become bus unavailable shall react such that:

- If a bus becomes unavailable and the node is not ready to sleep, the NM shall not enter bus sleep mode by itself.
- If a bus becomes unavailable and the node is ready to sleep, the NM shall enter bus sleep mode by itself.
- If a bus is unavailable and the node changes its state to ready to sleep, the NM shall enter bus sleep mode by itself.
- If a bus is unavailable and the node changes its state to not ready to sleep, the NM shall not enter bus sleep mode by itself.

The four rules in the description will make sure that the NM of a node that is currently not in bus sleep mode will never enter bus sleep mode while the node itself is not ready to sleep. If the node itself is ready to sleep, the NM shall enter bus sleep mode on its own.

NM of fault operation does not apply for a node that is already in bus sleep mode. In addition, bus unavailability may be hard to check at that time since the bus is not used to communicate in bus sleep mode.

2.9 ECU startup

The procedure for startup, see Figure 7.

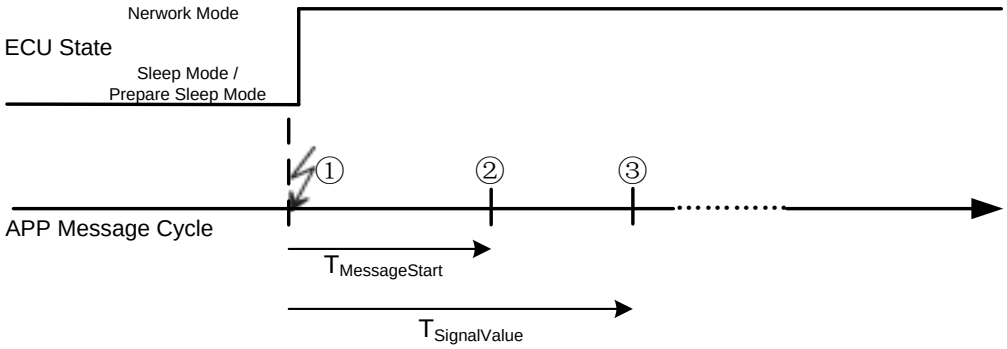

Figure 8 Start up Procedure

①: Local conditions active or received NM PDU.

②: ECU has transmitted all period and mixed messages at least once.

③: ECU transmits all signals with plausible values.

The timing parameters see Table 10.

Table 11 Start up Timing Parameter

Name	Unit	Min	Max	Comments
$T_{MessageStart}$	ms	0	300	Time frame within which all periodic and mixed messages have to be transmitted at least once.
$T_{SignalValue}$	ms	0	600	Time frame within which all signals shall have typically plausible values. In principle the signals shall have plausible values as soon as possible
Note : Any values defined by suppliers other than this range should be submitted to Geely in advance and be used after Geely's approval.				

3 Failure Mode Operation

When receiver nodes detect network fault, they all have to switch to system specific default value inputs for the function and continue the operation of functionality (if necessary, with reduced features). If required the functionality should also be switched off. DTC has to be recorded for the network fault.

The following faults shall be diagnosed by each ECU in the network:

- Lost communication detection
-CAN bus off fault
-Over/under voltage

3.1 Default Value and Substitute Value

For signal transmit/reception process, default value and substitute value shall be designed for each signal to be sent to CAN network or received from CAN network. Default values and substitute value shall be stored in ROM storage of CAN ECUs.

Two kinds of default value and substitute value shall be defined:

- **Default Value**:

  What is the default engineering value at start-up, so it also named as "**Default Value/at Start**.

  Serve as default value for receiving ECU's application when no signal is available from bus. Or serve as initial value which will be sent out to bus when no sampling/calculation result is available from sending ECU's application.

  This kind of default value is specified for each signal in CMX [2].

- **Error Substitute Value**

  The substitute value that is used when an error is confirmed. Typically, in case the needed signal reception is timeout and detected as loss signals, so it also named as "**Default Value/at Timeout**.

  For the received signals the user of the signals can specify which substitute value they need.

3.2 Lost Communication Detection

3.2.1 Lost Communication Detection Condition

Frame transmission detection shall be applied to all periodic or periodic &event type of transmissions. CAN frame is detected as LOST with following situations:

1) When it has not been received any one for continuously ***nbSuccLostFrame*** times of its periodic transmission time – Tx (defined in CMX) and the minimum time threshold of Lost communication detection shall be 250ms. See Table 11.

Table 12 Parameters on Frame Loss Detection-Timeout Value

Parameter	Symbol	Nominal	Unit	Comment
Time out of reception of needed periodic application frame after last reception of periodic frame by target ECU	nbSuccLostFrame[1)]	5*T	frame	T > 50ms *Tolerance 10%*
		250	ms	T ≤ 50ms *Tolerance 10%*
Note 1): If any deviation that shall be approved by Geely formally. *(E.g. maybe there is one very critical signal/message where the LOST signal detection shall be more precise than above....)*				

Table 13 Parameters on Frame Loss Detection-Diagnostic Enable Timer

Name	Unit	Min	Max	Comments
$T_{DiagEnable}$	s	3	4	Time since the KL15 is switched on to DTC Manager for detecting Lost Communication enable.

3.2.2 Lost Communication Self-Diagnosis

Once frame loss detection is valid under following conditions, DTC Communication Loss of each reception ECU shall be set in target ECU non-volatile memory:

- Voltage supply of CAN Bus node is in the range of **9-16V** (refer to communication diagnostic voltage definition for detail).
- The condition of $\mathbf{T_{DiagEnable}}$ is met.
- No Bus-off detected, and exceeding 1000ms after the last Bus-off recovery.
- Ignition state shall be IGN ON [1)].

ECU's relevant Communication Loss DTC is described in [3].

Note[1)]: If Lost communication self-diagnosis was done in any other states except IGN ON that shall be approved by Geely formally.

3.2.3 CAN Communication error Diagnosis

DTC Communication error include alive counter error, checksum error and DLC<8 error, it shall be stored in ECU non-volatile memory:

- Voltage supply of CAN Bus node is in the range of **9-16V** (refer to communication diagnostic voltage definition for detail).
- The condition of $\mathbf{T_{DiagEnable}}$ is met.
- No Bus-off detected, and exceeding 1000ms after the last Bus-off recovery.
- Ignition state shall be IGN ON.
- The Alive Counter error or checksum error or DLC<8 error detected is equal to 10.

ECU's relevant Communication Loss DTC is described in [3].

3.3 CAN BUS-OFF Handling

For this section, please differentiate between a “bus off state” in the CAN controller and a “bus off repair procedure” that is controlled by the application. A “bus off state” refers to a CAN controller state that ceases message transmission when the error counter exceeds 255 and is controlled by the CAN controller hardware. Whereas a “bus off repair procedure” is an application controlled procedure that shall be implemented through software.

3.3.1 CAN Application Frame Status — BUS-OFF

In case of ECU enters Bus-Off state, the periodic and event frame shall not be transmit on CAN Bus. Any remaining periodic and event frame waiting in Tx buffer shall be cleared by ECU application. And no transmission requests are allowed to be pending and resuming if transmission is enabled again.
After Bus-Off recovery and ECU back in network active state, periodic and event frame transmission shall be proceed again with the latest state of the signal.

3.3.2 CAN BUS-OFF Handling and Recovery

In case of the fatal bus error detection, any node shall restart the CAN controller initialization for a BUS recovery using following strategy illustrated in figure 8 and all Bus-off recovery parameters defined in table 13 which shall be applied by an ECU on CAN Bus.
The Bus-Off handling is a complicate process. By using the combined way of fast recovery and slow recovery processing is required in vehicle network. Bus-Off handing procedure describe as below:

- As long as Bus-Off detected by CAN controller and the Bus-Off flag will be set.
- Node will disconnect from the CAN bus as quickly as possible**,** when the Bus-Off event is indicated either by an interrupt or by a status bit that is polled in upper software.
- Reset CAN controller registers.
- All CAN communication should be paused in **tBusOffRecoveryL1 or tBusOffRecoveryL2.**
- When the timer of **tBusOffRecoveryL1 or tBusOffRecoveryL2** is expired, the node will (re)start trying to connect CAN bus.
- The initial value of **cL1ToL2** is zero. Once Bus-Off detected by CAN controller, the value of the **cL1ToL2** shall be plus one, at the same time the node will disconnect from the CAN bus. If the value of **cL1ToL2** increase to 11, it will no longer increase.
- The **tBusOffRecoveryL1** should be enable when the value of **cL1ToL2** less than or equal 10.
- When the value of **cL1ToL2** greater than 10, the **tBusOffRecoveryL2** shall be start and the **tBusOffRecoveryL1** should be stopped.
- When one of the messages was successfully transmitted, the network state of node should go back to available, i.e. the node will exit Bus-Off handing procedure and return to normal operation, and the value of **cL1ToL2** shall be cleared.

- If successful transmission of messages are not possible and the Bus-Off event is indicated again, the node should be retry to “bus off handing procedure” until the fault is cleared.

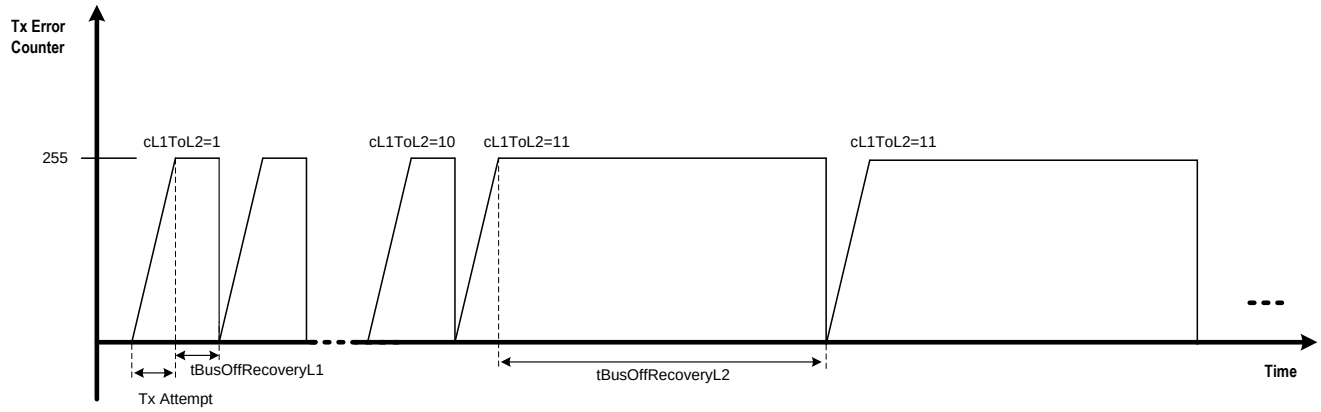

Figure 9 CAN Bus-Off recovery strategy

The parameters of Bus Off are described in table 13:

Table 14 CAN Bus Off Recovery Parameters

Parameter	Symbol	Min	Nominal	Max	Unit	Comment
Bus Off Recovery Time Level 1	tBusOffRecoveryL1	-	100	-	ms	This time parameter defines in milliseconds the duration of the bus-off recovery time in level 1 (short recovery time). *Tolerance 10%*
Bus Off Recovery Time Level 2	tBusOffRecoveryL2	-	1000	-	ms	This time parameter defines in milliseconds the duration of the bus-off recovery time in level 2 (long recovery time). *Tolerance 10%*
Bus Off counter L1 to L2	cL1ToL2		10			This threshold defines the count of bus-offs until the bus-off recovery switches from level 1 (short recovery time) to level 2 (long recovery time).

NOTE:

- The BUS-Off node retried delay timer (tBusOffRecoveryL1 or tBusOffRecoveryL2) shall be immediately (re)started after the CAN controller was reset by application program.
- Node disconnected from BUS: frame transmission stops and lost frame detection timer stops.
- Node connected to BUS: frame transmission is possible and lost frame detection timer activates.

- Receiving activity is enabled only after the CAN controller has left its internal bus off error state after 128 occurrences of 11 consecutive recessive bits have been seen on the bus.
- All the parameters were defined above shall be configurable.

3.3.3 CAN BUS-OFF Self-Diagnosis

DTC_BUS_OFF shall be stored in ECU non-volatile memory for entry of network Bus-Off state under following condition:

- Voltage supply of CAN Bus node is in the range of **9-16V** (refer to communication diagnostic voltage definition for detail)**.**
- The Bus Off counter cL1ToL2 is equal to 10.
- Ignition state shall be IGN ON.

ECU's relevant DTC_BUS_OFF are described in [3].

Note: This DTC_BUS_OFF log means is only recommendation, if some ECUs have different handling should be apply for Geely.

3.4 Under/Over Voltage Strategy

DTC_ Under/Over Voltage will be stored in ECU non-volatile memory, Under/Over Voltage detection is valid under following conditions:

- Voltage supply of CAN Bus node is≤ 9V(Under Voltage Strategy) , ≥16V(Over Voltage Strategy) (refer to communication diagnostic voltage definition for detail)**.**
- Battery voltage≤ 9V or battery voltage≥16V, keep the status at least 1s.
- Ignition state shall be IGN ON.

ECU's relevant DTC_ Under/Over Voltage are described in [3].

4 Communication diagnostic voltage

When the ECU detects over voltage or under voltage, it should follow the requirements be showed in figure10 and table15.

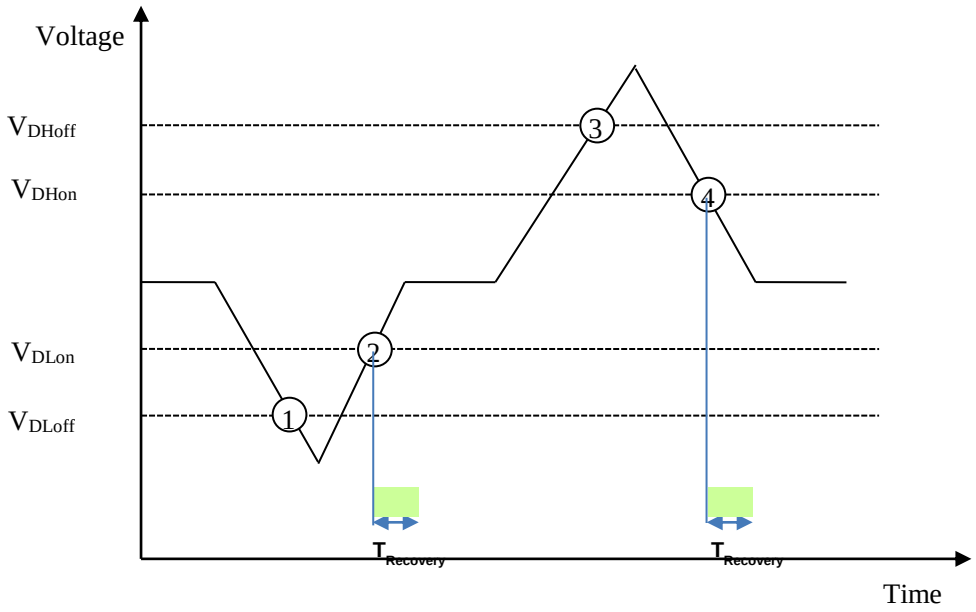

Figure10 The network related diagnostic during over voltage or under voltage

Table15 Network Diagnostic Voltage Range

Voltage value name	Typical[V]	Tolerance[V]
V_{DLon}	10	±0.5
V_{DLoff}	9	±0.5
V_{DHon}	15	±0.5
V_{DHoff}	16	±0.5

Table16 Network Diagnostic Timing Design

Timer name	Value [ms]	Tolerance
$T_{Recovery}$	500	±10%

Note：Any values defined by suppliers other than this range should be submitted to Geely in advance and be used after Geely's approval.

Transition – normal to under voltage

When battery voltage is showing decreasing trend (e.g. the voltage gradient dV/dt is negative) and voltage comes to the operating point①, all ECUs should stop the network related diagnosis immediately.

Transition – under voltage to normal

When battery voltage comes to the operating point② from the low battery voltage（precondition is the power supply voltage should within the range of the ECU able to work）, all ECUs should start the

under voltage recovery timer $T_{Recovery}$. After this timer $T_{Recovery}$ crosses, all ECUs should start the network related diagnosis. The timer should be reset when the voltage falls below V_{DLoff}.

Transition – normal to over voltage

When battery voltage is showing increasing trend (the voltage gradient dV/dt is positive) and voltage comes to the operating point ③, all ECUs should stop the network related diagnosis immediately.

Transition – over voltage to normal

When battery voltage comes to the operating point ④, all ECUs should start the over voltage recovery timer $T_{Recovery}$. After this timer $T_{Recovery}$ crosses, all ECUs should start the network related diagnosis. The timer should be reset when the voltage goes above V_{DHoff}.