Great Wall

GWMLAN General Specification

End-to-End Communication Protection Specification

Author	Zhao Haiyang
Approver	Wang Lichong

Confidentiality
Information in this document is the sole property of GWM and must not be disclosed to any third party without the prior written permission from GWM.

Revision History
Revision history describes the changes in the new issue. Please refer to the release notes.

Contents

1 Introduction

This document specifies the E2E protection mechanisms for functional safety, adequate for safety-related communication having requirements up to ASIL D. By using E2E protection mechanisms, the faults in the communication link can be detected and handled at runtime.

It is based on the GWMLAN concept by GWM and is adapted to the network for GWM project. It is adapted to the message that is related with the communication protection, whether or not it is related to functional safety.

1.1 Overview

The concept of E2E (end to end) communication protection is that safety-related data shall be protected during data tramsmission by encoding data at a sender (e.g., adding CRC, counter and data ID) and decoding the data at its associated receivers for checking the data integrity.

The medium between the 2 ends (sender and receiver) is treated as a black channel(see Figure 1), where systematic faults (e.g., design or implementation faults of communication related SW stack). Lower communication layers, and random hardware faults introduced by the MCU hardware, communication peripherals, transceivers, communication lines or other communication infrastructure could take place and eventually lead to a communication failure.

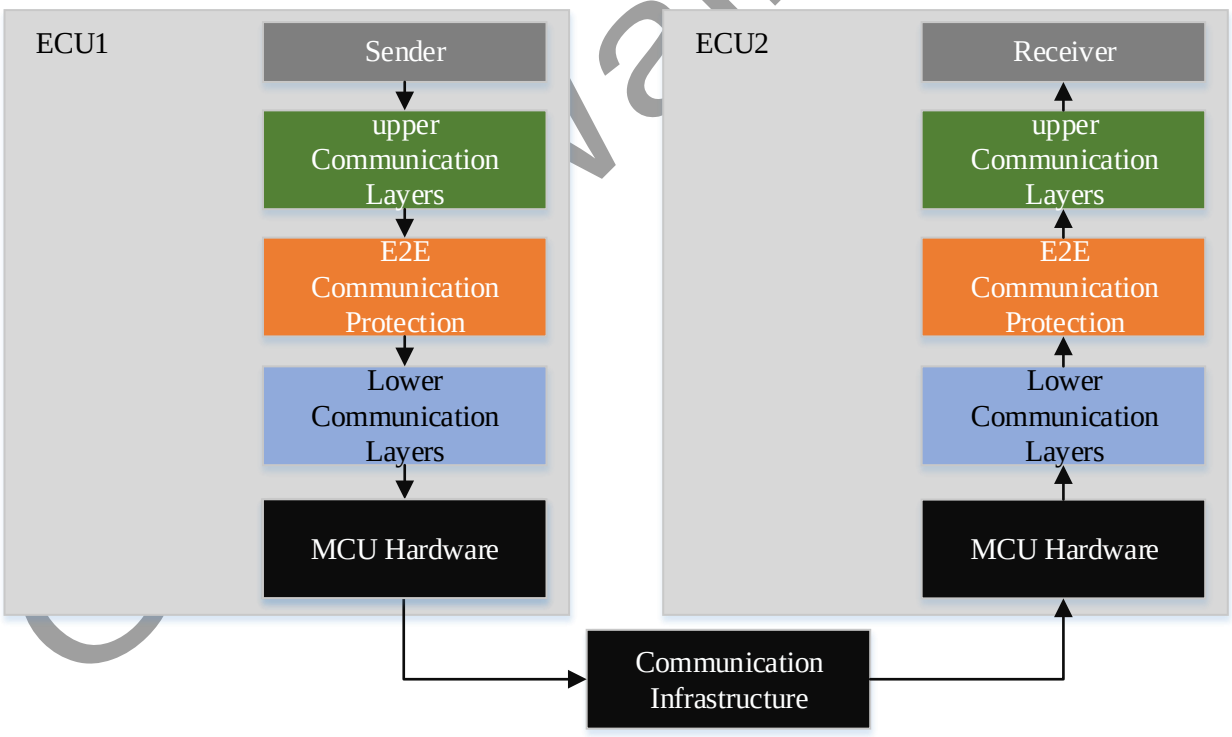

Figure1 Overview of E2E communication protection between a sender and a receiver

The E2E communication protection mechanism shall detect failure modes information loss, information delay, information corruption, information repretition, information insertion, incorrect information sequence, incorrect addressing of information at each target receiver.

AUTOSAR standard proposes 8 communication profiles (1, 2, 4, 5, 6, 7, 11 and 22) for E2E

communication protection. Generally, it works by adding control fields such as CRC, counter and data ID at the sender, and one or more receivers will evaluate the control fields to check the information integrity.

Depending on the system, GWM selects which E2E Profile is to be used from the E2E Profiles that provided by E2E Supervision.

Requirements can be identified by the "RS-E2E-id" unique string in front of each requirement.

1.2 Target Group/Purpose

This document specifies E2E communication protection mechanisms, faults in lower software and hardware layers can be detected and handled at runtime. In order to comply with ISO 26262 requirements up to ASIL D. This document specifies how to use and configure the E2E safety mechanisms provided by AUTOSAR within GWM infrastrucutre.

1.3 Terminology

CAN	Controller Area Network
C-Matrix	Communication Matrix
Data ID	An identifier that uniquely identifies the message
ECU	Electronic Control Unit, in general context
E2E	Short name for the End-to-End Communication Protection
GWM	Great Wall Motor
GWMLAN	GWM Local Area Network
HS-CAN	High Speed CAN
ASIL	Automotive Safety Integrity Level
CRC	Cyclic Redundancy Check

1.4 Document references

[1] 《AUTOSAR_SWS_E2ELibrary_V4.3.1》
[2] 《AUTOSAR_SWS_CRCLibrary_V4.3.1》

2 End to End communication protection

2.1 Generic requirements

RS-E2E-1

Every message which can have an influence on a safety goal rated with ASIL A, B, C or D, being periodically send through untrusted communication channel shall be protected via E2E Safety Mechanisms.

RS-E2E-2

Every message which can have an influence on a safety goal rated with ASIL A, B, C or D, received from untrusted communication channel shall be checked for it's integrity and reciever shall be informed about the integrity status (State->Status) as specified in AUTOSAR_SWS_E2ELibrary.
Note1: For more details, see respective E2E_Check chapters.
Note2: Every reciever entity will define it's actions based on the State->Status. For example for any other Status than "OK", reciever will consider recieved data as invalid.

RS-E2E-3

The integrity of implemented E2E Safety Mechanisms (on both, sender and reciever side) shall be at least the highest ASIL of all respective Safety Goals.
Note1:In case lower ASIL is used (e.g. ASIL B in case of ASIL B(D) requirement), it shall be argumented via additional safety analysis (e.g. no common cause failure between decomposed channels - different RTE stacks).

RS-E2E-4

Each message which is going to be protected via E2E Safety Mechanism, shall have assigned vehicle wide unique identification (DATA ID) as specified in AUTOSAR E2E Protocol Specification.
Note: For DATA ID length, see details for used Profile as specified in AUTOSAR E2E Protocol Specification.

RS-E2E-5

The reciever shall periodically poll for the payload integrity status (State->State), (regardless if new message is delivered or not), in order to detect timing-related faults such as delay or message loss.

RS-E2E-6

In the black channel (as described above in 1.1), there shall not be any possibility that any function can generate a valid E2E information (e.g., with correct data ID, CRC and counter).
Note: This in particular applies to QM gateways - they shall not be able to generate a valid E2E information.
E.g. if the lower communication layer (QM) would have a function which could analyze the information format and possibly corrupt the payload data but update a correct CRC in the information, the receiver could not detect such corruption in the black channel and will assume that the payload is valid after information integrity checking even if it's corrupted in the black channel.

RS-E2E-7

In case 8-bit CRC is used in the E2E (e.g. Profile 1), the reciever shall tolerate one undetected incorrect data payload (because CRC is generally not strong enough to ensure that every single corrupted message is detected) without violating any Safety Requirement or Goal.
Note: This requirements shall be also considered for other profiles (specially in case of ASIL (C), D

requirements) in case of considerably high failure rate on the communication channel.

2.2 Configure requirements

RS-E2E-8

For CAN/CANFD/LIN communication channel, the length of the complete Data (including application data,CRC and counter) not exceed 32 bytes shall be protected via E2E profile1.

RS-E2E-9

For profile1, GWM usage configuration:

Table 1 E2E Profile 1 configuration

Attribute	Value	Comment
profileName	PROFILE_1	Profile 1
crcOffset	0	CRC offset
counterOffset	56	Counter offset
Data_ID mode	DATA_ID_BOTH	both two bytes (double ID configuration) are included in the CRC
maxDeltaCounter	2	Maximum jump to be OK is 2, i.e. one lost message.
minOkStateInit	1	At least one OK message
maxErrorStateInit	1	One error allowed
windowSize	3	Last 3 messages are considered
minOkStateValid	1	At least one OK message
maxErrorStateValid	1	One error allowed
minOkStateInvalid	2	At least two OK messages
maxErrorStateInvalid	1	One error allowed
upperHeaderBitsToShift	0	no bits are shifted
SignalIPdu.unusedBitPattern	0xFF	unused places filled with 0xFF
profileBehavior	R4_2	Behavior of Profile P1 adjusted for the state machine.
maxNoNewOrRepeatedData	14	Behavior of Profile P1 adjusted for the state machine.
syncCounterInit	1	Behavior of Profile P1 adjusted for the state machine.

RS-E2E-10

E2E Profile 1 shall use the Crc_CalculateCRC8 function of the SWS CRC Supervision for calculating the CRC (CRC-8-SAE J1850).

Note1: For more details, see AUTOSAR_SWS_CRCLibrary.

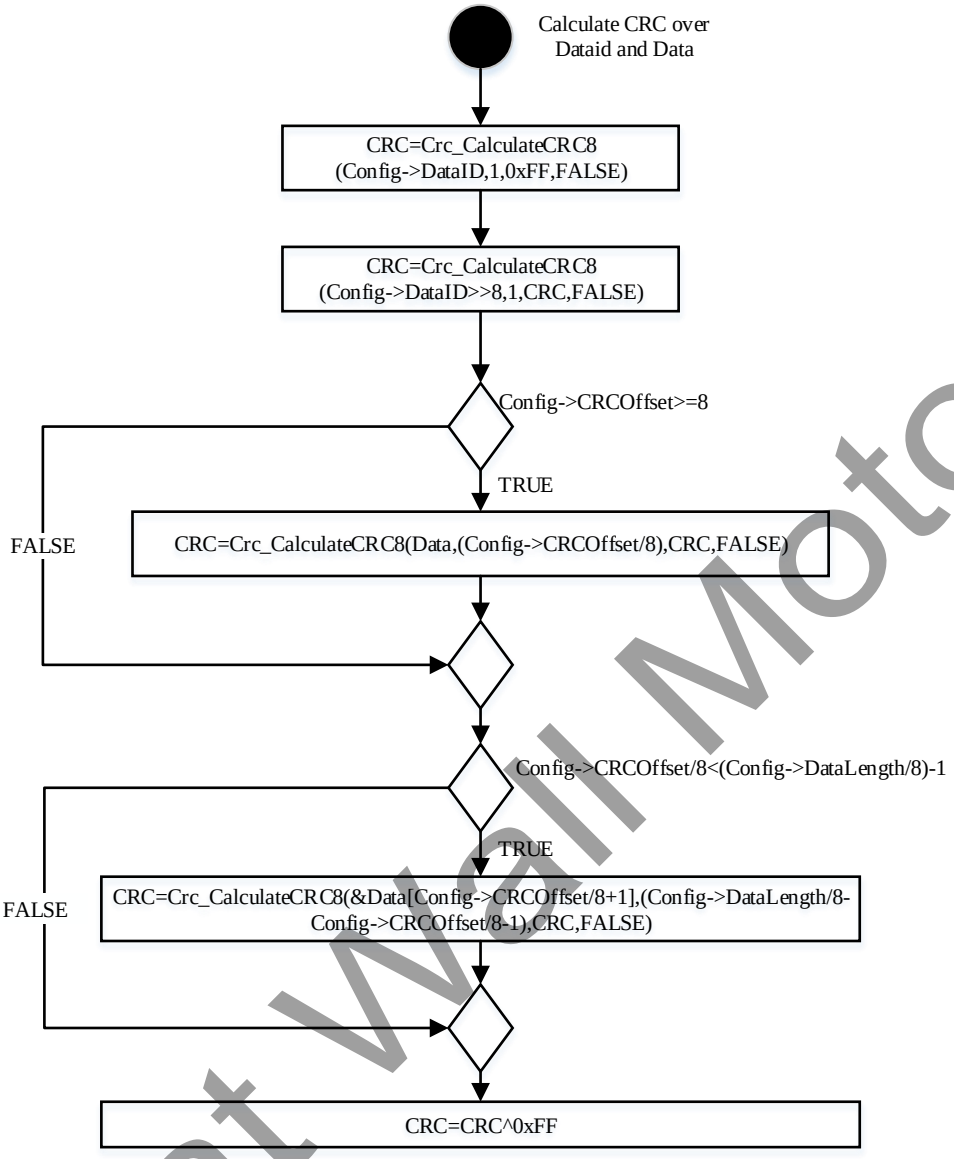

Figure 1 Subdiagram "Calculate CRC over Data ID and Data"

If E2E verification needs to be developed at the application layer, CRC verification needs to be developed as shown in Figure 1.

The algorithm can refer to the following example：

The value of the POLY is 0x1D.
The initial value of CRC signal is 0x00.

```
for( byte_index=1; byte_index< 10; ++byte_index )
  {
    CRC ^= data_byte_array[byte_index];
    for( bit_index=0; bit_index<8; ++bit_index )
        {
         if( (CRC & 0x80) != 0 )
         CRC = (CRC << 1) ^ POLY;
         else
         CRC = (CRC << 1);
```

```
        }
    }
```

CRC= CRC^0x00

The message data is CRC 0x00 0x00 0x00 0x00 0x00 0x00 0x00
DATA ID is 0x01(High byte) 0x23(Low byte)
Data_byte_array=0x23 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
After calculation, the CRC value is 0xCC.

RS-E2E-11

CRC algorithms (if any) used by communication stacks to minimize bus failure rate, shall use different CRC Polynomials than in used E2E mechanism.

Rationale: increase the error detection rate.

Note: In general it is also allowed to choose faster debouncing strategies than defined below (e.g. to react already on 1st valid message), as long as it is respectivily analyzed from safety point of view as acceptable and agreed with GWM respective safety responsible.

RS-E2E-12

E2E protects whole CAN message or segment of CANFD. If unused bits are replaced in a later point by a signal, then all receivers of that message that use the E2E need to be updated. As an alternative, ECUs should define dummy signals (and corresponding data elements) for all unused areas within message.

Sender： If message is protected by E2E, all unused bits and bytes shall be defined as dummy signals. Each bit of the dummy signal is set to zero before calculation of the CRC. Each bit of the dummy signal sent to the bus needs to be kept set to 0.

Receiver： If the received message is protected by E2E, all unused bits and bytes shall be defined as dummy signals. The receiver performs CRC calculation according to the actual received value on the bus. Any bits in the message is not allowed to be filled with 0 or 1 before calculation of the CRC.

2.3 Additional requirements

RS-E2E-13

Unless there is an argumentation for not to do so, the E2E communication protection shall be implemented by E2E transformer (a standardized way to invoke E2E) specified in AUTOSAR Specification of Module E2E Transformer and it shall be invoked internally by RTE.

RS-E2E-14

The debounce times of fault messages shall be considered within respective technical safety concept when estimating Fault Handling Time Interval.

RS-E2E-15

The receiver application shall perform correct reactions according to faults detected by E2E

protection.

Implementation hints:

Logical aspect: the reaction shall consider if it can mitigate or eliminate the fault effect at the system level, and ensure the system can enter and maintain at a state in which the system is still safe.

Timing aspect: the execution time of the reaction shall be less than defined fault reaction time. This is to ensure the reaction can be performed on time, avoiding to violate the FTTI.

3 Conflicts and issues

If conflicts are found between this specification and AUTOSAR E2E libray specification, then the specification should take the priority.

If the other issues are found during implementation process, you should trust the latest issues.

Revised record:

Version	Author	Date	Revised Description	Document maturity (draft/release)
1.0	Peng Jianli	2015-12-14	First Issue	released
1.1	Peng Jianli	2015-12-21	-Revise the 4.2、4.3、4.4 to adapt to the new scheme.The new algorithm will check all the signals which is raleated with the functional releated message.	released
1.2	Peng Jianli	2016-01-19	-Revise the "byte_index< 8" to " byte_index< 7" in 4.3 -Revise the "byte_index< 9" to "byte_index<8" in 4.4	released
1.3	Peng Jianli	2016-01-30	-Revise the "the data_byte_array is 9" to "the data_byte_array is 8" in 4.4 -Revise the "C-Matrix for HS-CAN" to "C-Matrix for project CHB071EAD" in 1.4 -Revise the "《Specification of SW-C End-to-End Communication Protection Library 4.0.3》" to "《AUTOSAR_SWS_E2ELibrary_4.0.3》" in 1.4.	released
1.4	Peng Jianli	2016-03-09	-Revise " So the length of the data_byte_array is 9" to " So the length of the data_byte_array is 8".	released
1.5	Fu Qiang	2016-11-04	-Add "Example" in 4.3 CRC without Data ID and 4.4 CRC with Data ID .	released
1.6	Zhao Haiyang	2018-12-29	- Change document name from"*Safety-related Mechanism Specification for CAN Communication*" to "*End-to-End Communication Protection Specification*". - Revise the section "*1.1 Overview"* and"*1.2 Target Group/Purpose"*. - Add "*Data ID/E2E/ASIL*" to the table in 1.3. - Revise the section"*1.4 Document references*". - Delete the section "*2 Counter*""*3 Timeout*" "*4 Checksum*". - Add the section"*2.End to End communication protection*".	released
1.7	Zhao Haiyang	2019-5-20	-Change RS-E2E-6"*counteroffset*"to 56 in Table 1. -Delete RS-E2E-6 "*dataIdNibbleOffset"* "*dataIdMode*" in Table 1.	released

1.8	Zhao Haiyang	2019-10-11	-Change section "*1. Introduction".* -Add "*For CAN/CANFD/LIN communication channel*" in RS-E2E-5.	released
1.9	Zhao Haiyang	2019-11-30	-Add"Data_ID mode" in Table 1 E2E Profile 1 configuration -Add CRC subdiagram and example in RS-E2E-7.	released
2.0	Zhao Haiyang	2019-12-28	-Add CRC algorithm example in RS-E2E-7	released
2.1	Zhao Haiyang	2020-5-21	-Add RS-E2E-12 in section 2.2 Configure requirements.	released