Elektrobit

EB tresos® Safety E2E Profile VCC safety manual

Date: 2019/07/11, ID: ASCE2ESE-336, Version 1.1, Status: accepted

Elektrobit Automotive GmbH
Am Wolfsmantel 46
91058 Erlangen, Germany
Phone: +49 9131 7701 0
Fax: +49 9131 7701 6333
Email: info.automotive@elektrobit.com

Technical support

https://www.elektrobit.com/support

Legal disclaimer

Confidential information.

Table of Contents

1. Document History 4
2. Introduction 5
3. Additional E2EPM Safety Mechanisms 6
    3.1. Proprietary E2E Profile VCC 6
    3.2. Protection of pure Intra-ECU Communication with Proprietary E2E Profile VCC 7
    3.3. Specification of AUTOSAR E2E Description 8
Glossary 10
Bibliography 11

1. Document History

Version	Date	Status	Description
V1.0.0	2014/02/24	PROPOSED	Initial version of safety manual extension for E2E Profile VCC.
V1.0.1	2014/02/28	PROPOSED	Added references to external documents.
V1.0.2	2014/03/07	PROPOSED	rework from inspection findings.
	2014/03/10	ACCEPTED	set to accepted: ASCE2ESE-17
V1.0.3	2014/04/11	PROPOSED	re-integration from branch
	2014/04/11	ACCEPTED	set to accepted: ASCE2ESE-389
V1.0.4	2014/05/20	PROPOSED	Fix incorrect definition of CRC Initial value.
	2014/11/06	accepted	set to accepted: ASCE2ESE-414
v1.1	2019/07/11	accepted	Update document title and name

Table 1.1. Document history

2. Introduction

This document is an extension to chapter "E2EPM Safety Mechanisms" of the delivered document "EB tresos® Safety E2E Wrapper safety manual" and specifies the proprietary E2E Profile VCC according to [XREF_E2EProtection] and additional clarification stated in [XREF_E2E_VCC_COMMENTS].

3. Additional E2EPM Safety Mechanisms

3.1. Proprietary E2E Profile VCC

[EB_E2ESE003292]

This profile is based on a customer request (ASR 4.0 Rev 3 [ASR_E2E_403], VCC Document [XREF_E2EProtection], and VCC-17-E2E-comments [XREF_E2E_VCC_COMMENTS]) and uses the following safety mechanisms:

- **CRC:** 8-bit CRC is explicitly sent with polynomial 0x1D (Initial value: 0x00, final XOR-value: 0x00). There is no constraint on the position of the CRC in the transmitted data.
- **Sequence/Alive counter:** A 4-bit sequence number (Counter representing numbers from 0 to 14) is explicitly sent and incremented at every transmission request. The bit-offset of the Sequence/Alive counter value for the CRC calculation is the low nibble of the first Byte used in the CRC calculation (high nibble is assumed to be 0). There is no constraint on the position of the Counter in the transmitted data.
- **System-wide unique 16-bit data ID for every port data element sent over a port:** The following data ID inclusion mode is used:
  - **Both bytes**: Both bytes of the 16-bit data ID are attached to the safety data for CRC calculation, but not explicitly sent.

The Figure 3.1, “Layout of the protected message for calculating the CRC value.” shows the serialized layout of the ProfileVCC used for CRC calculation only.

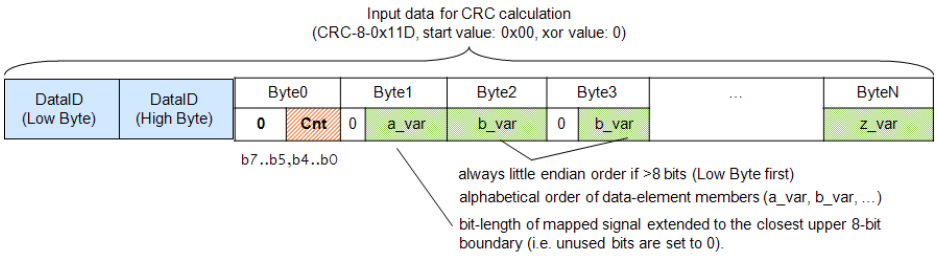

Figure 3.1. Layout of the protected message for calculating the CRC value.

[EB_E2ESE003293]

The serialization of the data into a byte array for CRC calculation shall be as follows:

- There shall exist no unused bits for the CRC calculation (i.e. bit-position equals bit-position plus bit-length of previously serialized data-element member).
- The bit-length of a data-element member is assumed to equal the size specified for the mapped group signal in the System Description, extended to the closest upper 8-bit boundary (i.e. unused bits are set to 0).

- CRC = CRC(DataIdLowByte,DataIdHighByte,CounterValue,Data1,Data2,...,DataN)

  whereas DataX corresponds to the individual bytes of the alphabetically ordered data-element members (name of the C-struct member) in little-endian order (if bit-length is greater than 8).

The Table 3.1, “Failure modes detection matrix for E2E Profile VCC” shows the failure modes and the required safety mechanisms of E2E Profile 1 with the different data ID variants for detection of the failure mode. Note: The different data ID inclusion modes only limits the applicable range of data IDs which can be used to detect Masquerading.

An 'X' specifies that the failure mode can be detected by the safety mechanism implemented in the E2E Profile.

An (X) specifies a safety mechanism which is only required to implement another safety mechanism.

An 'A' specifies that the failure mode can be detected by a safety mechanism implemented in the data sink.

Failure Mode \ Safety Mechanism	Sequence counter	CRC	data ID	Timeout detection	Range check
Unintended message repetition	X				
Message loss	X			A	
Insertion of message	X	(X)	X		
Resequencing	X				
Message corruption		X			X
Delayed reception				A	
Addressing faults	(X)	(X)	X		
Masquerading	(X)	(X)	X		

Table 3.1. Failure modes detection matrix for E2E Profile VCC

3.2. Protection of pure Intra-ECU Communication with Proprietary E2E Profile VCC

The protection of an intra-ECU communication is done in the same way like for profiles with configurable positions of protection information as stated in chapter "Protection of pure Intra-ECU Communication".

3.3. Specification of AUTOSAR E2E Description

Within the AUTOSAR Software Component Description (see [ASRSWSSWCT]), the E2E Description information for the protection with E2E Profile VCC is specified with the following string in the CATEGORY tag: ProfileVCC.

[EB_E2EPW020398]

The Communication Description shall be according to SWS Software Component Template [ASRSWSSWCT] with the following extensions for ProfileVCC:

- [EB_constr_1030] Existence of mandatory attributes

  Description:

  In the stated profile, the following attributes exist:

  - dataId: ALWAYS
  - dataIdMode: ALWAYS
  - crcOffset: ALWAYS in case of inter-Ecu communication only
  - counterOffset: ALWAYS in case of inter-Ecu communication only
  - maxDeltaCounterInit: OPTIONAL
  - maxNoNewOrRepeatedData: OPTIONAL
  - syncCounterInit: OPTIONAL
- [EB_constr_1031] Constraints for dataId

  Description:

  In the stated profile, the applicable range of values for dataId is [0 .. 65535].
- [EB_constr_1032] Constraints for dataIdMode

  Description:

  In the stated profile, the only allowed value for dataIdMode is 0 (Both data IDs used)
- [EB_constr_1034] Constraints of crcOffset

  Description:

  In the stated profile, the crcOffset shall be always [0 .. 65535].
- [EB_constr_1035] Constraints of counterOffset

  Description:

  In the stated profile, the counterOffset shall be always [0 .. 65535].

- [EB_constr_1036] Constraint of maxDeltaCounterInit

  Description:

  In the stated profile, the applicable range of values for maxDeltaCounterInit is [0 .. 14].
- [EB_constr_1037] Constraint of maxNoNewOrRepeatedData

  Description:

  In the stated profile, the applicable range of values for maxNoNewOrRepeatedData is [0 .. 14].
- [EB_constr_1038] Constraint of syncCounterInit

  Description:

  In the stated profile, the applicable range of values for syncCounterInit is [0 .. 14].

Glossary

Bibliography

[ASR_E2E_403] *AUTOSAR Specification of SW-C End-to-End Communication Protection Library, AUTOSAR_SWS_E2ELibrary, ASR 4.0 Rev 3* , 2011

[ASRSWSSWCT] *AUTOSAR Specification of Software Component Template, V4.2.0, R3*

[XREF_E2E_VCC_COMMENTS] *E2E VCC Comments*
http://subversion.ebgroup.elektrobit.com/svn/autosar/asc_E2ESE/asc_E2ESEExt/trunk/DAI/VCC-17-E2E-comments-VCC.pdf

[XREF_E2EProtection] *E2E PROTECTION CONCEPT*
http://subversion.ebgroup.elektrobit.com/svn/autosar/asc_E2ESE/asc_E2ESEExt/trunk/DAI/E2E Protection.doc