



Elektrobit

EB tresos[®] Safety E2E Profile 11 safety manual

Date: 2022-10-18, ID: EBASCE2E-961, Document version 0.3, Status: Released



Elektrobit Austria GmbH
Kaiserstraße 45
1070 Wien, Austria
Phone: +43 1 599 83 0
Fax: +43 1 599 83 18
Email: info.automotive@elektrobit.com

Technical support

<https://www.elektrobit.com/support>

Legal disclaimer

Confidential information.

ALL RIGHTS RESERVED. No part of this publication may be copied in any form, by photocopy, microfilm, retrieval system, or by any other means now known or hereafter invented without the prior written permission of Elektrobit Automotive GmbH.

All brand names, trademarks, and registered trademarks are property of their rightful owners and are used only for description.

Copyright 2023, Elektrobit Automotive GmbH.

Table of Contents

1. Document history	4
2. Document information	5
2.1. Objective	5
2.2. Scope and audience	5
2.3. Quality and safety statement	5
2.4. Motivation	5
2.5. Structure	5
2.6. Typography and style conventions	6
3. About EB tresos Safety E2E Profile 11	8
3.1. Architecture of the surrounding system	8
3.2. Description of E2EP11	8
3.2.1. Identification of E2EP11	8
3.2.2. What EB tresos Safety E2E Profile 11 does not do	8
4. Using EB tresos Safety E2E Profile 11 safely	9
4.1. Correct use and integration of the Safety E2E Profile 11	9
5. Safety element out of context (SEooC) definition	10
5.1. Assumed safety requirements of EB tresos Safety E2E Profile 11	10
5.2. Safety mechanism used by EB tresos Safety E2E Profile 11	10
5.2.1. Safety mechanisms	10
5.2.2. Failure modes and required safety mechanisms	12
6. Configuration verification criteria	14
A. Document configuration information	16
Bibliography	17

1. Document history

The author of the document as a whole is always Elektrobit Automotive GmbH.

Version	Date	State	Description
0.1	2021-11-03	Draft	Initial version
0.1	2021-11-17	Released	set to released, ASCE2E-961
0.2	2022-09-15	Released	set to released, ASCE2E-1062
0.3	2022-10-18	Released	set to released, ASCE2E-1098

Table 1.1. Document history

2. Document information

2.1. Objective

The objective of this document is to provide you with all the information necessary to ensure that EB tresos Safety E2E Profile 11 is used in a safe way.

2.2. Scope and audience

This safety manual describes the usage of E2EP11 in system applications which have safety requirements up to ASIL-D. It is valid for all projects and organizations which use E2EP11 in a safety-related environment. E2EP11 is intended to be used in AUTOSAR ECU projects.

The intended audience of this document is:

Professionals in embedded automotive systems with the appropriate qualification in the area of functional safety, communication networks, and AUTOSAR.

2.3. Quality and safety statement

Information about the quality level and safety status of E2EP11 release is provided in the quality statement. If such a statement is not available the software shall be considered as prototype level and must not be used in mass production projects.

2.4. Motivation

This safety manual provides the information on how to correctly use EB tresos Safety E2E Profile 11. This safety manual is an extension to the EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#) and all assumptions of this EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#) shall be fulfilled.

2.5. Structure

[Chapter 2, "Document information"](#) (this chapter) gives a brief description of the document structure.

[Chapter 3, “About EB tresos Safety E2E Profile 11”](#) describes E2EP11 in particular.

[Chapter 4, “Using EB tresos Safety E2E Profile 11 safely”](#) describes how to use E2EP11 safely.

[Chapter 5, “Safety element out of context \(SEooC\) definition”](#) describes the application constraints and the assumed requirements.

[Appendix A, “Document configuration information”](#) provides information about the document configuration.

Finally, the bibliography lists the documents that are referenced in the text.

2.6. Typography and style conventions

The signal word *WARNING* indicates information that is vital for the success of the configuration.

WARNING



Source and kind of the problem

What can happen to the software?

What are the consequences of the problem?

How does the user avoid the problem?

The signal word *NOTE* indicates important information on a subject.

NOTE



Important information

Gives important information on a subject

The signal word *TIP* provides helpful hints, tips and shortcuts.

TIP



Helpful hints

Gives helpful hints

Throughout the documentation, you find words and phrases that are displayed in **bold**, *italic*, or `monospaced` font.

To find out what these conventions mean, see the following table.

All default text is written in Arial Regular font.

Font	Description	Example
Arial italics	Emphasizes new or important terms	The <i>basic building blocks</i> of a configuration are module configurations.
Arial boldface	GUI elements and keyboard keys	1. In the Project drop-down list box, select Project_A. 2. Press the Enter key.
Monospaced font (Courier)	User input, code, and file directories	The module calls the BswM_Dcm_RequestSessionMode() function. For the project name, enter Project_Test.
Square brackets []	Denotes optional parameters; for command syntax with optional parameters	insertBefore [<opt>]
Curly brackets { }	Denotes mandatory parameters; for command syntax with mandatory parameters	insertBefore {<file>}
Ellipsis ...	Indicates further parameters; for command syntax with multiple parameters	insertBefore [<opt>...]
A vertical bar	Indicates all available parameters; for command syntax in which you select one of the available parameters	allowinvalidmarkup {on off}

3. About EB tresos Safety E2E Profile 11

E2EP11 provides a consistent set of data protection mechanisms that protect against the faults considered along the communication path, including random hardware faults and systematic software faults.

3.1. Architecture of the surrounding system

The architecture of the surrounding system is described in the EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#).

3.2. Description of E2EP11

3.2.1. Identification of E2EP11

E2EP11 is composed of the `E2EP11` module itself, the E2E Protection Profile 11 documentation [\[E2EP11UG\]](#) and the safety manual (this document).

3.2.2. What EB tresos Safety E2E Profile 11 does not do

You should only use EB tresos Safety E2E Profile 11 together with EB tresos Safety E2E Transformer (E2E). If you use EB tresos Safety E2E Profile 11 without EB tresos Safety E2E Transformer (E2E), you are responsible to integrate EB tresos Safety E2E Profile 11 to your system according to the ISO 26262.

4. Using EB tresos Safety E2E Profile 11 safely

EB tresos Safety E2E Transformer (E2E) is developed as a safety element out of context (SEooC). Therefore, Elektrobit Automotive GmbH assumes that the environment meets particular requirements so that the E2EP11 code behaves appropriately and safely.

For more information on intended usage and possible misuse of E2EP11, see the EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#) and the E2E Protection Profile 11 documentation [\[E2EP11UG\]](#).

4.1. Correct use and integration of the Safety E2E Profile 11

- The Configuration should be done in ARXML file

5. Safety element out of context (SEooC) definition

EB tresos Safety E2E Transformer (E2E) is defined as SEooC. For more information, see the EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#).

5.1. Assumed safety requirements of EB tresos Safety E2E Profile 11

The assumed safety requirements for the selected product are defined in the EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#).

5.2. Safety mechanism used by EB tresos Safety E2E Profile 11

5.2.1. Safety mechanisms

This profile bases on E2E Profile 11 specified by AUTOSAR, see [\[ASR_E2E_430\]](#). It is called from the virtual functional bus generated by the `Rte` module together with a previously called serializing transformer, e.g. `ComXf`, or `SomeIpXf`) to add protection information to the serialized data stream for the following communication paradigms:

- ▶ Non-blocking queued sender-receiver communication:

`E2EP11` provides APIs to add protection information on the sender side to the result of a serializing transformer, e.g. `ComXf` or `SomeIpXf`. It also provides APIs to cyclically check communication errors by using this information on the receiver side. The `E2EXf` module calls the API functions. The bit-offset of the CRC value within a transmitted signal group is configurable but must be byte-aligned.

The `E2EP11` module uses the following safety mechanisms:

- ▶ **Cyclic redundancy check (CRC):** An 8-bit CRC is explicitly sent with polynomial in normal form `0x1D` with an initial value `0xFF` and a final XOR-value `0xFF`.

- ▶ **Sequence counter/alive counter:** A 4-bit sequence number with a counter that represents numbers from 0 to 14 is explicitly sent and incremented at every transmission request. The bit-offset of the sequence counter/alive counter value within a transmitted signal group is configurable but must be aligned with respect to nibbles.
- ▶ **System-wide unique 16-bit data ID for every port data element sent over a port:** The following data ID inclusion modes can be configured:
 - ▶ **Both bytes** E2E_P11_DATAID_BOTH (variant 11A, dataIdMode=0): Both bytes of the 16-bit data ID are attached to the safety data for CRC calculation but not explicitly sent.
 - ▶ **Alternating bytes** E2E_P11_DATAID_ALT (variant 11B, dataIdMode=1): The low and the high byte are alternating attached to the safety data for CRC calculation depending on the parity of the counter, but not explicitly sent.
 - ▶ Even counter values include the low byte.
 - ▶ Odd counter values include the high byte.
 - ▶ **Explicit transmission of data ID nibble** E2E_P11_DATAID_NIBBLE (variant 11C, dataIdMode=3): Both bytes of the 16-bit data ID are attached to the safety data for CRC calculation, but the low nibble of the high byte of the data ID is explicitly transmitted. Only 12 bits are used in this 16-bit data ID, and the high nibble of the high byte is set to 0. The bit-offset of the data ID nibble value within a transmitted signal group is configurable, but must be aligned with respect to nibbles. To use this data ID inclusion mode together with the data ID inclusion mode **both bytes**, the CRC is calculated over the low byte of the data ID and the high byte, which is set to 0. For more information on explicit transmission of data ID nibbles, see [Figure 5.3, “Layout of the protected message including control data \(CRC, SEQ\) with explicit transmission of data ID nibble \(dataIdMode=3\)”](#). The constraints specified in ASR_-E2EP11020541 must be adhered to.

[Figure 5.1, “Layout of the protected message including control data \(CRC, SEQ\) with 2-byte data ID \(dataIdMode=0\)”](#) shows the layout of the AUTOSAR E2E Profile 11 with a CRC offset of 0 bits and a sequence counter/alive counter offset of 8 bits for dataIdMode=0.

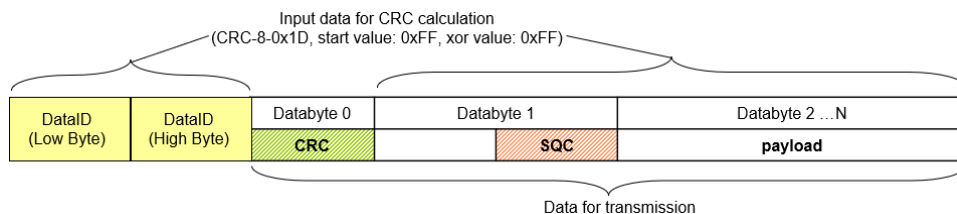


Figure 5.1. Layout of the protected message including control data (CRC, SEQ) with 2-byte data ID (dataIdMode=0)

[Figure 5.2, “Layout of the protected message including control data \(CRC, SEQ\) with 2-byte data ID \(dataIdMode=1\)”](#) shows the layout of the AUTOSAR E2E Profile 11 with a CRC offset of 0 bits and a sequence counter/alive counter offset of 8 bits for dataIdMode=1.

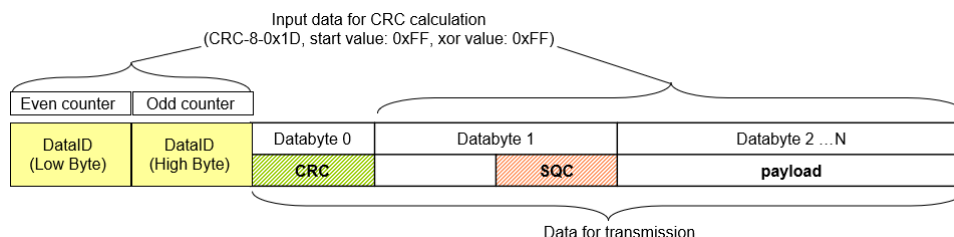


Figure 5.2. Layout of the protected message including control data (CRC, SEQ) with 2-byte data ID (`dataIdMode=1`)

Figure 5.3, “Layout of the protected message including control data (CRC, SEQ) with explicit transmission of data ID nibble (`dataIdMode=3`)” shows the layout of the AUTOSAR E2E Profile 11 with a CRC offset of 0 bits and a sequence counter/alive counter offset of 8 bits and a data ID nibble offset of 12 bits as used for `dataIdMode=3`.

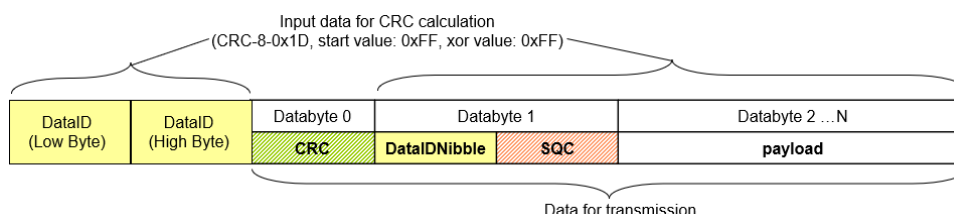


Figure 5.3. Layout of the protected message including control data (CRC, SEQ) with explicit transmission of data ID nibble (`dataIdMode=3`)

5.2.2. Failure modes and required safety mechanisms

The serialization of the application data is equal to the layout of the corresponding signal group for all variants. [Table 5.1, “Failure modes detection matrix for E2E Profile 11”](#) shows the failure modes and the required safety mechanisms of E2E Profile 11 with the different data ID variants for detection of the failure mode.

NOTE

Different data ID inclusion modes



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 is detectable by the safety mechanism implemented in the E2E Profile.

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

An **A** specifies that the failure mode is detectable by a safety mechanism implemented in the data sink.

Failure mode/ safety mechanism	Sequence counter	CRC	Data ID	Timeout detection
Unintended message repetition	X			

Failure mode/ safety mechanism	Sequence counter	CRC	Data ID	Timeout detection
Message loss	X			A
Insertion of mes- sage	X	(X)	X	
Resequencing	X			
Message corruption		X		
Delayed reception				A
Addressing faults	(X)	(X)	X	
Masquerading	(X)	(X)	X	

Table 5.1. Failure modes detection matrix for E2E Profile 11

6. Configuration verification criteria

This chapter lists checks that you must perform manually.

[ASR_E2EP11_020071]

Verify that every protected data element has a unique data ID within one implementation of a communication network.

[ASR_E2EP11_020308]

Verify that the following applies for Profile 11 in the nibble data ID configuration:

- ▶ The high nibble of the high byte of the data ID is equal to 0.
- ▶ The low nibble of the high byte of the Data ID is within the range 0x1 . . 0xE, to avoid collisions with other E2E Profile 11 configurations that have 0x0 on this nibble and to exclude the invalid value 0xF.
- ▶ The low byte of the data ID is different to the low byte of any data ID present in the same bus that uses an E2E Profile in the double data ID configuration.

[ASR_E2EP11_020072]

Verify that under the assumption of two data elements DE1 and DE2 on the same system (vehicle), for any data element DE1 that has ASIL B, ASIL C, or ASIL D requirements with data ID DI1, there shall not exist any other data element DE2 (of any ASIL) with data ID DI2, where: `Crc_CalculateCRC8(start value: 0xFF, data[2]: {lowbyte (DI1),highbyte(DI1)}) = Crc_CalculateCRC8(start value: 0xFF, data[2]: {lowbyte (DI2),highbyte(DI2)})`.

Note: The requirement shown above limits the usage of data IDs of data having ASIL B, C, and D to 255 distinct values in a given ECU. This gives the flexibility to define the data IDs within the 16-bit naming space.

[ASR_E2EP11_020073]

Verify that under the assumption of two data elements, DE1 and DE2, on the same system (vehicle), for any data element DE1 that has ASIL A requirements with data ID DI1, there shall not exist any other data element DE2 (that has ASIL A requirements) with data ID DI2 and of the same length as DE1, where `Crc_CalculateCRC8(start value: 0xFF, data[2]: {lowbyte (DI1),highbyte(DI1)}) = Crc_CalculateCRC8(start value: 0xFF, data[2]: {lowbyte (DI2),highbyte(DI2)})`.

Note: Fulfilled by the user's guide.

[ASR_E2EP11_020317]

Verify that the following shall be respected when E2E Profiles E2E_P11_DATAID_BOTH (variant 11A) and E2E_P11_DATAID_NIBBLE (variant 11C) are used in one bus/system:

- ▶ E2E_P11_DATAID_BOTH (variant 11A) data shall use IDs that are < 256, this means the high byte shall always be = 0.
- ▶ E2E_P11_DATAID_NIBBLE (variant 11C) data shall use IDs that are >= 256, this means the high byte is always != 0 and < 4096 (0x1000 - it means they fit to 12 bits).

- Any low byte of the E2E_P11_DATAID_NIBBLE (variant 11C) data ID shall be different to any low byte of the E2E_P11_DATAID_BOTH (variant 11A) data ID.

The requirement showed above allows data ID distribution and the detection of addressing errors. In particular, these can be detected when an E2E_P11_DATAID_NIBBLE (variant 11C) message arrives at an E2E_P11_DATAID_BOTH (variant 11A) destination. For instance, if an E2E_P11_DATAID_BOTH (variant 11A) destination receives an E2E_P11_DATAID_NIBBLE (variant 11C) message, the CRC check will pass if the low byte of the sent E2E_P11_DATAID_NIBBLE (variant 11C) message equals to the expected E2E_P11_DATAID_BOTH (variant 11A) address. The requirement shown above excludes this case.

Example: Under the assumption that there are 200 used E2E_P11_DATAID_BOTH (variant 11A) data IDs, this requirement allows the use of additionally $(256-200)*15 = 840$ data IDs.

Example: E2E_P11_DATAID_BOTH (variant 11A) may use addresses 0 to 199, while E2E_P11_DATAID_NIBBLE (variant 11C) may use addresses where the low byte is 200 to 255 and the high byte is between 1 and 15.

Appendix A. Document configuration information

This document was created by the DocBook engine using the source files and revisions listed below. All paths are relative to the directory https://subversion.ebgroup.elektrobit.com/svn/autosar/asc_E2E/asc_E2EP11/stable/RFI_ACG-8.8.7_Safety_2/doc/public/safety_manual.

Filename	Revision / Hash
../../../../asc_E2ESEXfmgmt/doc/public/fragments/Bibliography.xml	5067
document.ent.m4	5458
EB_tresos_Safety_E2E_Profile_11_safety_manual.xml	5458
SM_Assumed_Requirements.xml	6282
SM_Bibliography.xml	5458
SM_ConfigCriteria.xml	6282
SM_Description.xml	6174
SM_Document_information.xml	5458
SM_Glossary.xml	5458
SM_History.xml	6285
SM_SafeUse.xml	6282

Bibliography

[ASR_E2E_430] *AUTOSAR Specification of SW-C End-to-End Communication Protection Library AUTOSAR_SWS_E2ELibrary, ASR 4.3.0 ,*

[E2EP11UG] *E2E Protection Profile 11 documentation:*

**[SM_-
ASCE2ESE-519]** *EB tresos Safety E2E Transformers safety manual*