



Elektrobit

EB tresos[®] Safety E2E Profile 1 safety manual

Date: 2021-04-07, ID: EBASCE2E-401, Document version 0.6, 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 2021, 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 1	8
3.1. Architecture of the surrounding system	8
3.2. Description of E2EP01	8
3.2.1. Identification of E2EP01	8
3.2.2. What EB tresos Safety E2E Profile 1 does not do	8
4. Using EB tresos Safety E2E Profile 1 safely	9
5. Safety element out of context (SEooC) definition	10
5.1. Assumed safety requirements of EB tresos Safety E2E Profile 1	10
5.2. Safety mechanism used by EB tresos Safety E2E Profile 1	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
Glossary	17
Bibliography	18

1. Document history

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

Version	Date	State	Description
0.1	2017-02-13	Draft	Initial version
0.2	2017-03-17	Proposed	Add configuration verification criteria
0.3	2017-03-23	Proposed	Update due to review findings
0.3	2018-01-19	Released	set to released, ASCE2E-401
0.4	2019-04-15	Draft	Add quality and safety statement
0.5	2019-07-15	Released	set to released, ASCE2E-779
0.6	2021-04-07	Released	Implemented profile E2EP01B

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 1 is used in a safe way.

2.2. Scope and audience

This safety manual describes the usage of E2EP01 in system applications which have safety requirements up to ASIL-D. It is valid for all projects and organizations which use E2EP01 in a safety-related environment. E2EP01 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 E2EP01 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 1. This safety manual is an extension to the [Generic E2E products safety manual](#) and all assumptions of this [Generic E2E products safety manual](#) 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 1”](#) describes E2EP01 in particular.

[Chapter 4, “Using EB tresos Safety E2E Profile 1 safely”](#) describes how to use E2EP01 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 1

E2EP01 provides a consistent set of data protection mechanisms, which are designed to 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 depends on which AUTOSAR serialization mechanism is selected. You can use E2EP01 either by EB tresos Safety E2E Wrapper or EB tresos Safety E2E Transformer (E2E). When E2EP01 is embedded in EB tresos Safety E2E Wrapper then the surrounding system is described in the EB tresos Safety E2E Wrapper safety manual [\[EBASCE2ESE-16\]](#) and if EB tresos Safety E2E Transformer (E2E) is used then the surrounding system is described in the EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#).

3.2. Description of E2EP01

3.2.1. Identification of E2EP01

E2EP01 is composed of the E2EP01 module itself, the Documentation [\[E2EP01UG\]](#) and the safety manual (this document).

3.2.2. What EB tresos Safety E2E Profile 1 does not do

You should only use EB tresos Safety E2E Profile 1 together with one of the two products EB tresos Safety E2E Wrapper or EB tresos Safety E2E Transformer (E2E). If you use EB tresos Safety E2E Profile 1 without one of these two EB products, you are responsible to integrate EB tresos Safety E2E Profile 1 to your system according to the ISO 26262.

4. Using EB tresos Safety E2E Profile 1 safely

EB tresos Safety E2E Wrapper and EB tresos Safety E2E Transformer (E2E) are developed as a safety element out of context (SEooC). Therefore, Elektrobit Automotive GmbH assumes that the environment meets particular requirements so that the E2EP01 code behaves appropriately and safely.

For more information on intended usage and possible misuse of E2EP01, see the [Generic E2E products safety manual](#) and the Documentation [\[E2EP01UG\]](#).

5. Safety element out of context (SEooC) definition

EB tresos Safety E2E Wrapper and EB tresos Safety E2E Transformer (E2E) are defined as SEooC. For more information, see the [Generic E2E products safety manual](#).

5.1. Assumed safety requirements of EB tresos Safety E2E Profile 1

The assumed safety requirements for the selected product are either defined in the EB tresos Safety E2E Wrapper safety manual [\[EBASCE2ESE-16\]](#) or the EB tresos Safety E2E Transformers safety manual [\[SM_ASCE2ESE-519\]](#) depending in which combination you use EB tresos Safety E2E Profile 1.

5.2. Safety mechanism used by EB tresos Safety E2E Profile 1

5.2.1. Safety mechanisms

This profile is based on E2E Profile 1 specified by AUTOSAR, see [\[ASR_E2E_403\]](#) and [\[ASR_E2E_421\]](#). E2EP01 uses the following safety mechanisms:

- ▶ **Cyclic redundancy check (CRC):** An 8-bit CRC is explicitly sent with polynomial $0x1D$ with an initial value $0x00$ and a final XOR-value $0x00$. The bit-offset of the CRC value within a transmitted signal group is configurable but must be byte-aligned.
- ▶ **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** (dataIdMode=0): Both bytes of the 16-bit data ID are attached to the safety data for CRC calculation, but not explicitly sent.

- ▶ **One of the two bytes is included** (dataIdMode=1): Depending on parity of the counter (alternating ID configuration). For an even counter, the low byte and for an odd counter, the high byte is included. The length of the Data ID shall be 16 bits (i.e. 2 byte).
- ▶ **Low byte only** (dataIdMode=2): Only the low byte of the 16-bit data ID is attached to the safety data for CRC calculation, but not explicitly sent, while the high byte is set to 0.
- ▶ **Explicit transmission of data ID nibble** (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 be able 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 5.4, “Layout of the protected message including control data \(CRC, SEQ\) with explicit transmission of data ID nibble \(dataIdMode=3\)”](#). The constraints specified in ASR_E2EP01_020377 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 1 with a CRC offset of 0 bits and a sequence counter/alive counter offset of 8 bits for dataIdMode=0.

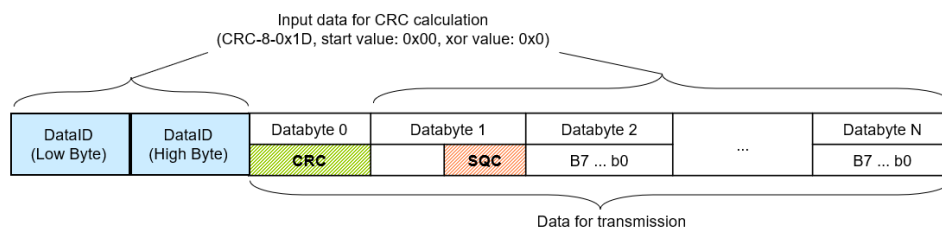


Figure 5.1. Layout of the protected message including control data (CRC, SEQ) with 2-byte data ID (dataIdMode=0)

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 1 with a CRC offset of 0 bits and a sequence counter/alive counter offset of 8 bits for dataIdMode=1.

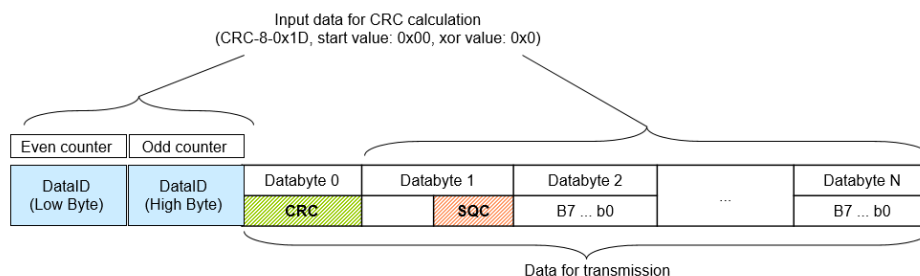


Figure 5.2. Layout of the protected message including control data (CRC, SEQ) with 2-byte data ID (dataIdMode=1)

Figure 5.3, “Layout of the protected message including control data (CRC, SEQ) with 1-byte data ID (`dataIdMode=2`)” shows the layout of the AUTOSAR E2E Profile 1 with a CRC offset of 0 bits and a sequence counter/alive counter offset of 8 bits for `dataIdMode=2`.

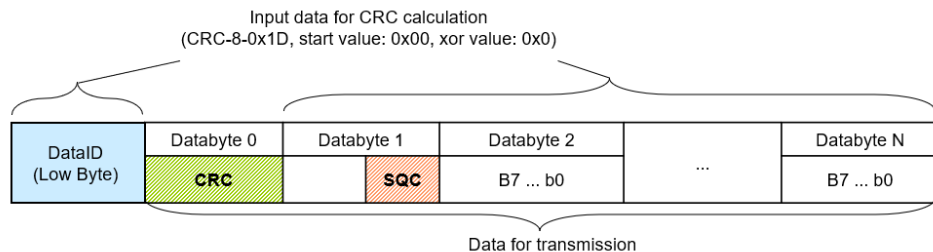


Figure 5.3. Layout of the protected message including control data (CRC, SEQ) with 1-byte data ID (`dataIdMode=2`)

Figure 5.4, “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 1 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`.

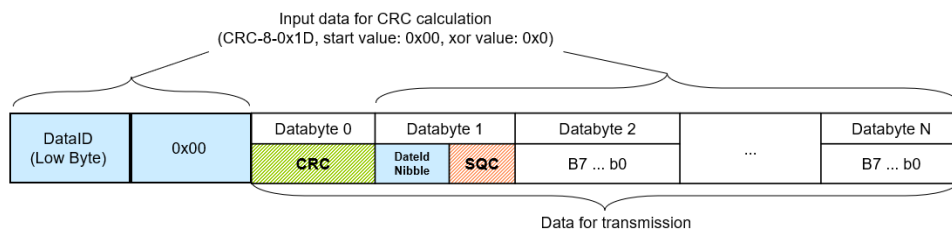


Figure 5.4. Layout of the protected message including control data (CRC, SEQ) with explicit transmission of data ID nibble (`dataIdMode=3`)

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 1” 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



Different data ID inclusion modes

The different data ID inclusion modes only limit 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.

A **W** specifies that the failure mode can be detected by the safety mechanism implemented in the product EB tresos Safety E2E Wrapper. If this module is used directly in the Software Component or is used together with a different product, e.g. EB tresos Safety E2E Transformer (E2E), ensure that either this safety mechanism is not required or already implemented in a different module, e.g. **Rte**.

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			W
Delayed reception				A	
Addressing faults	(X)	(X)	X		
Masquerading	(X)	(X)	X		

Table 5.1. Failure modes detection matrix for E2E Profile 1

6. Configuration verification criteria

This chapter lists checks that you must perform manually.

[ASR_E2EP01_020071]

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

[ASR_E2EPP01_020308]

Verify that the following applies for Profile 1 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 1 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_E2EP01_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 above requirement limits the usage of data IDs of data that have ASIL B, C, D to 255 distinct values in a given ECU, but gives the flexibility to define the data IDs within the 16-bit naming space.

[ASR_E2EP01_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_E2EP01_020377]

Verify that the following shall be respected, when E2E Profiles 1A and 1C are used in one bus/system:

- ▶ 1A data shall use IDs that are < 256, this means the high byte shall always be = 0.
- ▶ 1C 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 1C data ID shall be different to any low byte of the 1A data ID.

Thanks to the data ID distribution according to the above requirement, the addressing errors can be detected. In particular these can be detected when an 1C message arrives at an 1A destination. For example, if an 1C message is received at an 1A destination, the CRC check will pass if the low byte of the sent 1C message equals to the expected 1A address - and this is excluded by the above requirement. Example: Under the assumption that there are 200 used 1A data IDs, this requirement allows to use additional $(256-200)*15 = 840$ data IDs.

Example: 1A may use addresses 0 to 199, while 1C 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_E2EP01/stable/RFI_ACG-8.8.4-X3_1/doc/public/safety_manual.

Filename	Revision / Hash
../../../../../asc_E2ESEXfmgmt/doc/public/fragments/Bibliography.xml	4085
document.ent.m4	2745
EB_tresos_Safety_E2E_Profile_01_safety_manual.xml	2695
SM_Assumed_Requirements.xml	5161
SM_Bibliography.xml	2692
SM_ConfigCriteria.xml	2720
SM_Description.xml	2745
SM_Document_information.xml	4028
SM_Glossary.xml	2746
SM_History.xml	5161
SM_SafeUse.xml	2745

Glossary

Generic E2E Safety
Manual

E2EP01 can be used by EB tresos Safety E2E Wrapper or by EB tresos Safety E2E Transformer (E2E). If E2EP01 is used together with EB tresos Safety E2E Wrapper this safety manual is an extension to the chapter *Safety Mechanisms* of the [\[EBASCE2ESE-16\]](#) or if E2EP01 is used together with EB tresos Safety E2E Transformer (E2E) this safety manual is an extension to the chapter *Safety Mechanisms* of the [\[SM_ASCE2ESE-519\]](#).

Bibliography

- [ASR_E2E_403]** *AUTOSAR Specification of SW-C End-to-End Communication Protection Library, AUTOSAR_SWS_E2ELibrary, ASR 4.0 Rev 3 , 2011*
- [ASR_E2E_421]** *AUTOSAR Specification of SW-C End-to-End Communication Protection Library, AUTOSAR_SWS_E2ELibrary, ASR 4.2.1 ,*
- [E2EP01UG]** *Documentation: EB tresos E2E Profile 1*
- [EBASCE2ESE--16]** *EB tresos Safety E2E Wrapper safety manual*
- [SM_-
ASCE2ESE-519]** *EB tresos Safety E2E Transformers safety manual*