Elektrobit

EB tresos® Safety E2E Profile 4 safety manual

Date: 2020-10-27, ID: EBASCE2E-404, Document version 0.4, 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.

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 4 8
    3.1. Architecture of the surrounding system 8
    3.2. Description of E2EP04 8
        3.2.1. Identification of E2EP04 8
        3.2.2. What EB tresos Safety E2E Profile 4 does not do 8
4. Using EB tresos Safety E2E Profile 4 safely 9
5. Safety element out of context (SEooC) definition 10
    5.1. Assumed safety requirements of EB tresos Safety E2E Profile 4 10
    5.2. Safety mechanism used by EB tresos Safety E2E Profile 4 10
        5.2.1. Safety mechanisms 10
        5.2.2. Failure modes and required safety mechanisms 11
6. Configuration verification criteria 13
A. Document configuration information 14
Bibliography 15

1. Document history

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

Version	Date	State	Description
0.1	2017-05-20	Draft	Initial version
0.1	2018-01-19	Released	set to released, ASCE2E-404
0.2	2019-04-15	Draft	Add quality and safety statement
0.3	2019-07-15	Released	set to released, ASCE2E-779
0.4	2020-10-27	Released	Support for use cases with MaxDataLength up to 8kB, ASR_E2EP04_020072, set to released, ASCE2E-881

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 4 is used in a safe way.

2.2. Scope and audience

This safety manual describes the usage of E2EP04 in system applications which have safety requirements up to ASIL-D. It is valid for all projects and organizations which use E2EP04 in a safety-related environment. E2EP04 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 E2EP04 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 4. 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 4“ describes E2EP04 in particular.

Chapter 4, “Using EB tresos Safety E2E Profile 4 safely“ describes how to use E2EP04 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 *basic building blocks* 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 4

E2EP04 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 is described in the EB tresos Safety E2E Transformers safety manual [SM_ASCE2ESE-519].

3.2. Description of E2EP04

3.2.1. Identification of E2EP04

E2EP04 is composed of the `E2EP04` module itself, the E2E Protection Profile 4 documentation [E2EP04UG] and the safety manual (this document).

3.2.2. What EB tresos Safety E2E Profile 4 does not do

You should only use EB tresos Safety E2E Profile 4 together with EB tresos Safety E2E Transformer (E2E). If you use EB tresos Safety E2E Profile 4 without EB tresos Safety E2E Transformer (E2E), you are responsible to integrate EB tresos Safety E2E Profile 4 to your system according to the ISO 26262.

4. Using EB tresos Safety E2E Profile 4 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 E2EP04 code behaves appropriately and safely.

For more information on intended usage and possible misuse of E2EP04, see the EB tresos Safety E2E Transformers safety manual [SM_ASCE2ESE-519] and the E2E Protection Profile 4 documentation [E2EP04UG].

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 4

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 4

5.2.1. Safety mechanisms

This profile is based on E2E Profile 4 specified by AUTOSAR, see [ASR_E2E_421]. 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

  `E2EP04` provides APIs to add protection information at the sender to the result of a serializing transformer, e.g. `ComXf` or `SomeIpXf`. It also provides APIs to cyclically check for communication errors by using this information at the receiver. Its API functions are called by the `E2EXf` module.

The `E2EP04` module uses the following safety mechanisms:

- **Cyclic redundancy check (CRC):** A 32-bit CRC is explicitly sent with polynomial in normal form `0x1F4ACFB13` with an initial value `0xFFFFFFFF` and a final XOR-value `0xFFFFFFFF`.
- **Sequence counter/alive counter:** A 16-bit sequence number is explicitly sent and incremented at every transmission request.

- **Data ID:** A system-wide unique 32-bit data ID is explicitly sent for every port data element.
- **Length:** A 16-bit number to support dynamic-size data.

The header of AUTOSAR E2E Profile 4 can be placed at a specific location in the protected data, by configuring the offset of the entire E2E header. Figure 5.1, “Header layout of AUTOSAR E2E Profile 4.” shows the header layout with a header offset equal to `0`. The individual control data fields are encoded in Big Endian with the most significant byte first.

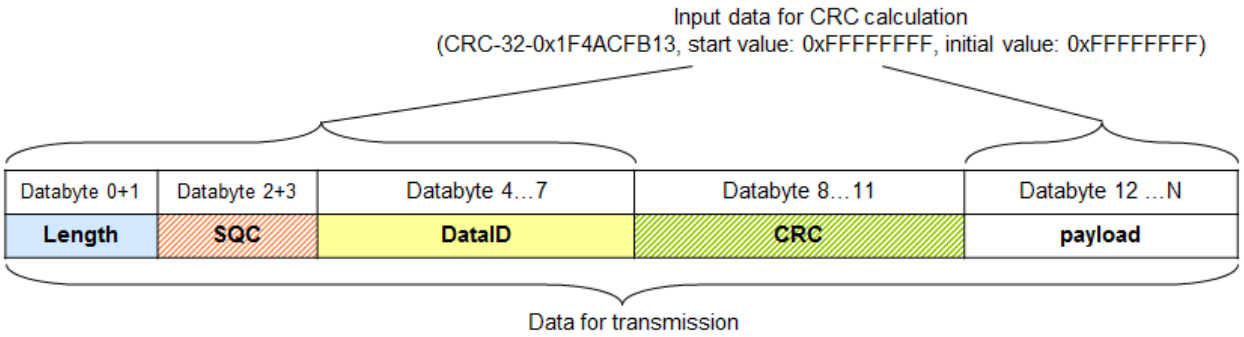

Figure 5.1. Header layout of AUTOSAR E2E Profile 4.

5.2.2. Failure modes and required safety mechanisms

Table 5.1, “Failure modes detection matrix for E2E Profile 4” shows the failure modes and the required safety mechanisms of E2E Profile 4 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 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
Unintended message repetition	X			
Message loss	X			A

Failure mode/ safety mechanism	Sequence counter	CRC	Data ID	Timeout detection
Insertion of message	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 4

6. Configuration verification criteria

This chapter lists checks that you must perform manually.

[ASR_E2EP04_020071]

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

[ASR_E2EP04_020072]

Verify that in case the checker reports a violation of MaxDataLength > 4KB that the selected value for the MaxDataLength is acceptable for your safety case.

Note: The recommended MaxDataLength is less than or equal to 4kB, according AUTOSAR. There might be use cases to have MaxDataLength up to 8kB with profile 4.

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_E2EP04/stable/RFI_ACG-8.8.5_Safety_1/doc/public/safety_manual.

Filename	Revision / Hash
../../../../asc_E2ESEXfmgmt/doc/public/fragments/Bibliography.xml	4749
document.ent.m4	2759
EB_tresos_Safety_E2E_Profile_04_safety_manual.xml	2759
SM_Assumed_Requirements.xml	2985
SM_Bibliography.xml	2759
SM_ConfigCriteria.xml	4805
SM_Description.xml	2987
SM_Document_information.xml	4028
SM_Glossary.xml	2759
SM_History.xml	4952
SM_SafeUse.xml	2759

Bibliography

[ASR_E2E_421] *AUTOSAR Specification of SW-C End-to-End Communication Protection Library, AUTOSAR_SWS_E2ELibrary, ASR 4.2.1* ,

[E2EP04UG] *E2E Protection Profile 4 documentation*:

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