Elektrobit

EB tresos® Safety E2E Profile 2 safety manual

Date: 2019-07-15, ID: EBASCE2E-403, 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

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

Version	Date	State	Description
0.1	2017-05-16	Draft	Initial version
0.2	2017-05-23	Proposed	Set state to proposed
0.2	2018-01-19	Released	set to released, ASCE2E-403
0.3	2019-04-15	Draft	Add quality and safety statement
0.4	2019-07-15	Released	set to released, ASCE2E-779

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 2 is used in a safe way.

2.2. Scope and audience

This safety manual describes the usage of E2EP02 in system applications which have safety requirements up to ASIL-D. It is valid for all projects and organizations which use E2EP02 in a safety-related environment. E2EP02 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 E2EP02 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 2. 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 2“ describes E2EP02 in particular.

Chapter 4, “Using EB tresos Safety E2E Profile 2 safely“ describes how to use E2EP02 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 2

E2EP02 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 E2EP02 either by EB tresos Safety E2E Wrapper or EB tresos Safety E2E Transformer (E2E). When E2EP02 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]. When 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 E2EP02

3.2.1. Identification of E2EP02

E2EP02 is composed of the `E2EP02` module itself, the E2E Protection Profile 2 documentation [E2EP02UG] and the safety manual (this document).

3.2.2. What EB tresos Safety E2E Profile 2 does not do

You should only use EB tresos Safety E2E Profile 2 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 2 without one of these two EB products, you are responsible to integrate EB tresos Safety E2E Profile 2 to your system according to the ISO 26262.

4. Using EB tresos Safety E2E Profile 2 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 E2EP02 code behaves appropriately and safely.

For more information on intended usage and possible misuse of E2EP02, see the *Generic E2E products safety manual* and the E2E Protection Profile 2 documentation [E2EP02UG].

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 2

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 2.

5.2. Safety mechanism used by EB tresos Safety E2E Profile 2

5.2.1. Safety mechanisms

This profile is based on E2E Profile 2 specified by AUTOSAR, see [ASR_E2E_403] and [ASR_E2E_421]. E2EP02 uses the following safety mechanisms:

- **Cyclic redundancy check (CRC):** An 8-bit CRC is explicitly sent with polynomial `0x2F` with an initial value `0xFF` and a final XOR-value `0xFF`.
- **Sequence counter/alive counter:** A 4-bit sequence number (SQC) is explicitly sent and incremented at every transmission request.
- **System-wide unique data ID list for every port data element sent over a port:** A list of 16 8-bit values where the sequence counter index is used to select the current data ID. The data ID is attached to the safety data for CRC calculation, but not explicitly sent.

Figure 5.1, “Layout of the protected message including control data (CRC, SQC)” shows the layout of the AUTOSAR E2E Profile 2.

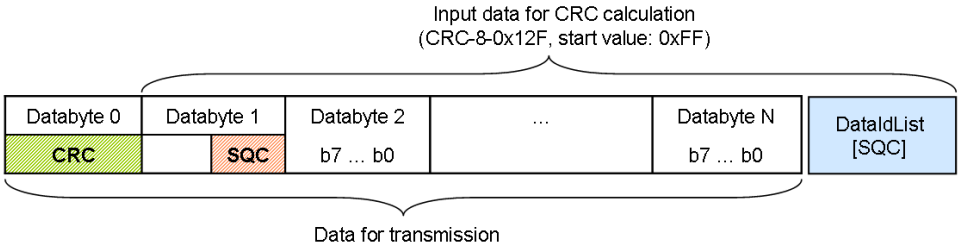

Figure 5.1. Layout of the protected message including control data (CRC, SQC)

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. Table 5.1, “Failure modes detection matrix for E2EP02” shows the failure modes and the required safety mechanisms of E2E Profile 2 for detection of the failure mode.

An `X` specifies that the safety mechanisms detects or contributes to the detection of the related failure mode.

An `(X)` specifies that the safety mechanism contributes to the detection of the related failure mode.

An `A` specifies that the failure mode is not detected directly by a detection mechanism of the E2E profile but can be detected at the receiver SW-C.

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	

Failure mode/safety mechanism	Sequence counter	CRC	Data ID	Timeout detection	Range check
Addressing faults	(X)	(X)	X		
Masquerading	(X)	(X)	X		

Table 5.1. Failure modes detection matrix for E2EP02

6. Configuration verification criteria

This chapter lists checks that you must perform manually.

[ASR_E2EP02_020071]

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

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_E2EP02/stable/RFI_ACG-8.8.0-X3_1/doc/public/safety_manual.

Filename	Revision
..\..\..\..\asc_E2ESEXfmgmt\doc\public\fragments\Bibliography.xml	4085
document.ent.m4	2747
EB_tresos_Safety_E2E_Profile_02_safety_manual.xml	2747
SM_Assumed_Requirements.xml	2989
SM_Bibliography.xml	2747
SM_ConfigCriteria.xml	2747
SM_Description.xml	2988
SM_Document_information.xml	4028
SM_Glossary.xml	2747
SM_History.xml	4237
SM_SafeUse.xml	2747

Glossary

`Generic E2E Safety Manual`	E2EP02 can be used by EB tresos Safety E2E Wrapper or by EB tresos Safety E2E Transformer (E2E). If E2EP02 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 E2EP02 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* ,

[E2EP02UG] *E2E Protection Profile 2 documentation*:

[EBASCE2ESE--16] *EB tresos Safety E2E Wrapper safety manual*

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