Document Title	Requirements on E2E Communication Protection
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	651

Document Status	Final
Part of AUTOSAR Standard	Classic Platform
Part of Standard Release	4.3.1

Document Change History

Date	Release	Changed by	Change Description
2017-12-08	4.3.1	AUTOSAR Release Management	• minor corrections / clarifications / editorial changes; For details please refer to the ChangeDocumentation
2016-11-30	4.3.0	AUTOSAR Release Management	• Update requirements considering new profiles 7, 11, 22 • Update requirements tracing
2014-10-31	4.2.1	AUTOSAR Release Management	• Initial release

Disclaimer

Table of Contents

1 Scope of Document

This document defines requirements on E2E Communication Protection according to ISO26262. These requirements shall be used as a basis for specification of detailed E2E mechanisms and their usage in AUTOSAR implementations up to ASIL D systems.

2 Conventions to be used

- The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078].

- In requirements, the following specific semantics shall be used (based on the Internet Engineering Task Force IETF).

  The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as:

  - SHALL: This word means that the definition is an absolute requirement of the specification.
  - SHALL NOT: This phrase means that the definition is an absolute prohibition of the specification.
  - MUST: This word means that the definition is an absolute requirement of the specification due to legal issues.
  - MUST NOT: This phrase means that the definition is an absolute prohibition of the specification due to legal constraints.
  - SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
  - SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
  - MAY: This word, or the adjective „OPTIONAL“, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation, which does include the option, though perhaps with reduced functionality. In the same vein an implementation, which does include a particular option, MUST be prepared to interoperate with another implementation, which does not include the option (except, of course, for the feature the option provides.)

3 Acronyms and abbreviations

All technical terms used in this document, except the ones listed in the table below, can be found in the official AUTOSAR glossary.

Abbreviation / Acronym:	***Description:***
E2E	End-to-End

4 Requirements tracing

Requirement	Description	Satisfied by
RS_BRF_00110	AUTOSAR shall offer methods to protect safety related data communication against corruption	SRS_E2E_08527, SRS_E2E_08528, SRS_E2E_08529, SRS_E2E_08530, SRS_E2E_08533, SRS_E2E_08536, SRS_E2E_08537, SRS_E2E_08539
RS_BRF_00113	AUTOSAR shall detect signal time-outs	SRS_E2E_08528, SRS_E2E_08529
RS_BRF_01056	AUTOSAR BSW modules shall provide standardized interfaces	SRS_E2E_08527, SRS_E2E_08538
RS_BRF_01280	AUTOSAR RTE shall offer the external interfaces between Software Components and between Software Components and BSW	SRS_E2E_08538
RS_BRF_02096	AUTOSAR shall provide checksum computation of cyclic redundancy check sums as a library	SRS_E2E_08533
RS_BRF_02104	AUTOSAR shall provide end-to-end protection support as a library	SRS_E2E_08527, SRS_E2E_08528, SRS_E2E_08529, SRS_E2E_08530, SRS_E2E_08531, SRS_E2E_08534, SRS_E2E_08536, SRS_E2E_08537, SRS_E2E_08539

5 Requirements Specification

In this chapter the requirements of both AUTOSAR modules E2E library and E2E transformer are specified.

5.1 Functional Overview

Safety-related automotive systems often use a safe data transmission to protect communication between components (as required by ISO 26262), which means that:

1. Communication errors shall be prevented (e.g. by means of appropriate software architecture and by means of verification)
2. If error prevention alone is insufficient (e.g. for inter-ECU communication), then the errors shall be detected at runtime to a sufficient degree (c.f. diagnostic coverage, safe failure fraction) and that the rate of undetected dangerous errors is below some allowed limit (c.f. residual error rate, probability of dangerous failure per hour or probability of dangerous failure on demand).

To provide a safe End-to-End communication between SW-Cs, a solution shall be integrated within the AUTOSAR methodology which does require no or low additional non-standard code (like wrappers above RTE).

The functionality of End-to-End communication protection is to be supported by the following AUTOSAR modules:

- E2E Library
- E2E Transformer

The E2E transformer provides

- Abstraction of communication in conformance to RTE API
- Protection of the serialized exchange of information that is exchanged by COM stack via RTE independent of RTE implementation and RTE internal data types
- Interface to E2E library

The E2E library provides

- The definition of profiles 1, 2, 4,5, 6, 7, 11 and 22 including check and protect functions.
- A state machine describing the logical algorithm of E2E monitoring independent of the used profile.

If these modules are used for communication protection RTE, Transformer, E2E Transformer, E2E Library, CRC Library, OS context switch and scheduling are assumed to be safety-related modules. Therefore, in a mixed ASIL environment, it has to be shown by a safety analysis, that QM or low ASIL software has no access to the E2E buffer so that freedom from interference can be ensured.

5.2 Functional Requirements

5.2.1 E2E transformer

E2E transformer is invoked via RTE and it is placed between the RTE and E2E Library. It is responsible for the configuration and state management of the E2E protection.

5.2.1.1 [SRS_E2E_08538] An E2E transformer shall be provided⌈

Type:	Valid
Description:	E2E transformer shall be provided which can be invoked via RTE and is placed between the caller (RTE) and E2E Library. It shall be responsible for the configuration and state management of the E2E protection and it shall provide a protection for messages serialized by at least Some/IP and COM-based transformer.
Rationale:	The whole complexity of the configuration and management of E2E Library stays within the E2E Transformer. Thanks to this, E2E protection can be realized without additional integrator code.
Use Case:	Communication between main chassis ECU SW-C and power steering ECU SW-C. Some/IP is a serialization protocol for Ethernet. COM-based transformers are typically used in CAN, FlexRay, CanFD
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01056, RS_BRF_01280)

5.2.2 E2E Library

E2E library provides a set of safety protocols, in a form of library functions invoked by SW-Cs. The protocols shall provide the error detection that is sufficient for transmitting safety-related data up to ASIL D, through a QM communication stack.
It provides:

1. E2E profiles 1, 2, 4, 5, 6, 7, 11, 22.
2. E2E state machine

5.2.2.1 [SRS_E2E_08528] E2E library shall provide E2E profiles, where each E2E profile completely defines a particular safety protocol⌈

Type:	Valid
Description:	E2E library shall provide E2E profiles, where each E2E profile completely defines a particular safety protocol (including header structure, behavior as state machines, error handling etc). Each E2E profile shall be an efficient solution for a particular AUTOSAR communication stack used underneath (which are Ethernet, FlexRay, CAN, CAN FD or LIN), and the ASIL rating of the exchanged signals. Note: Each communication stack (e.g. FlexRay) has different error rates which depend on for example: - Bit error rate on channel - FIT values of HW - number of ECUs

	- topology (e.g. CAN->Gateway->FR) - open/closed transmission system - frequency of safety related messages The profiles, based on proven-in-use solutions, are supposed to cover typical combinations of above factors.
Rationale:	Too many standardized profiles reduce interoperability between applications. Moreover, it introduces too much specification and development efforts.
Use Case:	Protocol with 8-bit CRC for CAN, and 16-bit for long FlexRay signals.
Dependencies:	--
Supporting Material:	--

](RS_BRF_02104, RS_BRF_00113, RS_BRF_00110)

5.2.2.2 [SRS_E2E_08527] E2E library shall provide E2E profiles, in a form of library functions[

Type:	Valid
Description:	E2E library shall provide a set of safety protocols, in a form of library functions. The protocols shall provide the error detection that is sufficient for transmitting safety-related data up to ASIL D, through a communication stack implemented as QM software.
Rationale:	E2E communication protection is state-of-art in automotive safety-related series products.
Use Case:	Communication between main chassis ECU SW-C and power steering ECU SW-C
Dependencies:	--
Supporting Material:	--

](RS_BRF_01056, RS_BRF_02104, RS_BRF_00110)

5.2.2.3 [SRS_E2E_08529] Each of the defined E2E profiles shall use an appropriate subset of specific protection mechanisms [

Type:	Valid
Description:	Each of the defined E2E profiles shall use an appropriate subset of the following mechanisms: 1. Sequence number (different sizes possible; in the state-of art it is alternatively called alive counter or consecutive number 2. CRCs of length: 8, 16, 32, 64 bits 3. IDs: Source ID, Destination ID, Data ID 4. Timeouts: reception timeout In other words, mechanisms not listed shall not be used. In each E2E profile, the sequence number and IDs, if used, should be all part of the transmitted data element. However, it is allowed that in a given profile, the sequence number and/or IDs are “hidden” (not transmitted), but included in the CRC.
Rationale:	These are typical measures used by safety protocols, and they can be realized by AUTOSAR.
Use Case:	Mechanisms used in an exemplary profile: 4-bit sequence counter, CRC8, Data ID, timeout
Dependencies:	--
Supporting Material:	--

](RS_BRF_02104, RS_BRF_00110, RS_BRF_00113)

5.2.2.4 [SRS_E2E_08530] Each E2E profile shall have a unique ID, define precisely a set of mechanisms and its behavior in a semi-formal way ⌈

Type:	Valid
Description:	Each E2Eprofile defined within the library shall: 1. Have a unique ID (IDs from E2E_01 to E2E_16 are reserved for standard AUTOSAR profiles). 2. Define precisely a set of mechanisms (e.g. CRC of a particular polynomial) 3. Define its behavior in a semi-formal way (including state machines, error handling etc).
Rationale:	A protocol is not just a list of mechanisms (e.g CRC8 + sequence number) , but the whole logic managing the process. Standardization of header is by far not sufficient. Standardized behaviour is needed to achieve interoperability.
Use Case:	Usually one state machine per profile per communicating partner (sender, receiver, client server) is sufficient. ECU1 and ECU2 communicating. ECU1 has different implementation of E2E library than ECU2.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02104, RS_BRF_00110)

5.2.2.5 [SRS_E2E_08531] E2E library shall call the CRC routines of CRC library

⌈

Type:	Valid
Description:	E2E library shall not provide CRC routine implementations. Instead, it shall call the CRC routines of CRC library (document UID 016).
Rationale:	Reuse of existing AUTOSAR functionality
Use Case:	CRC8 of CRC library to be used in one of profiles for protecting CAN communication.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02104)

5.2.2.6 [SRS_E2E_08533] CRC used in a E2E profile shall be different than the CRC used by the underlying physical communication protocol⌈

Type:	Valid
Description:	CRC used in each E2E profile shall be different than the CRC used by the underlying communication protocols (Wi-Fi, Ethernet, IP, UDP, TCP, FlexRay, CAN, CAN FD, LIN), for which the given profile is supposed to be used with.
Rationale:	Using the same polynomials twice (once in com stack and again in E2E) provides significantly lower joint detection rate than using two different polynomials. The polynomials available in AUTOSAR R3.1 are not optimal for E2E anyway.

Use Case:	If profile X is supposed to be used only for FlexRay, then its CRC shall be different than the one of FlexRay.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02096, RS_BRF_00110)

5.2.2.7 [SRS_E2E_08534] E2E library shall provide separate error flags and error counters for each type of detected communication failure ⌈

Type:	Valid
Description:	E2E library shall provide to the application layer separate errors flag and error counters for each type of detected communication failure. In other words if E2E profile X is supposed to use the sequence counter and CRC, then the following error flag shall be available to the application layer: • Data corruption • Wrong sequence • Repetition • Data loss
Rationale:	Error handling strategies are “application dependent”, and cannot be “a priory defined”
Use Case:	Enable error-dependent reaction of the SW-C using E2E library.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02104)

5.2.2.8 [SRS_E2E_08536] Either SW-C or E2E Library shall compute the intermediate CRC over application data element ⌈

Type:	Valid
Description:	Either SW-C or E2E Library shall compute the intermediate CRC over application data element. E2E library shall use as initial CRC value the intermediate CRC and shall compute the CRC over the sequence counter (if it is used) and IDs (if used).
Rationale:	In case of complex data elements, the E2E library cannot compute the CRC over the data element (because the library does not know the layout of the data element – a data type may be e.g. an array of pointers to data structures, which does not occupy a consecutive address space). In such a case, the application needs to compute the CRC over the data element, and pass the computed CRC to the library. However, regardless who invokes the CRC computation (SW-C or library), the CRC used is the one of the used E2E profile.
Use Case:	--
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02104, RS_BRF_00110)

5.2.2.9 [SRS_E2E_08537] When using E2E Profiles 1/2, SW-Cs shall tolerate at least one received data element that is invalid/corrupted but not detected by E2E

⌈

Type:	Valid
Description:	When using E2E Profiles 1/2, SW-Cs shall tolerate at least one received data element that is invalid/corrupted but not detected by E2E.
Rationale:	Requiring that 100% errors are detected by E2E protocol has high impact on implementation of E2E library (e.g. requiring SW or/and HW redundancy). Allowing to have a signal (in a sequence of received signals) with an error that is not detected by E2E
Use Case:	Example 1: multiple bit errors (e.g. 5 corrupted bits) that generate the same CRC as the original signal. Example 2: random HW fault or SW fault in E2E library causing that CRC Sequence Counter computation does not detect an error.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02104, RS_BRF_00110)

5.2.2.10 [SRS_E2E_08539] An E2E protection mechanism for inter-ECU communication of large data shall be provided

⌈

Type:	Valid
Description:	This E2E mechanism shall support protection of large, composite data with dynamic-length, of the length up to 4MB.
Rationale:	Large, composite data need specific protection mechanisms.
Use Case:	Communication between main chassis ECU SW-C and power steering ECU SW-C, communication of vision data, delivery of configuration data, delivery of flash software updates.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02104, RS_BRF_00110)

6 References

none