Document Title	Requirements on E2E
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	847

Document Status	Final
Part of AUTOSAR Standard	Foundation
Part of Standard Release	1.5.1

Document Change History

Date	Release	Changed by	Description
2019-03-29	1.5.1	AUTOSAR Release Management	• Functional overview: information added • Functional requirements: information added • New requirements added (RS_E2E_08544, RS_E2E_08545, RS_E2E_08546, RS_E2E_08547, RS_E2E_08548)
2018-10-31	1.5.0	AUTOSAR Release Management	• Editorial changes
2018-03-29	1.4.0	AUTOSAR Release Management	• No content changes
2017-12-08	1.3.0	AUTOSAR Release Management	• No content changes
2017-10-27	1.2.0	AUTOSAR Release Management	–Migration of document to standard "Foundation"– • Editorial changes
2017-03-31	17-03	AUTOSAR Release Management	• Initial release

Disclaimer

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work.

The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

This work may be utilized or reproduced without any modification, in any form or by any means, for informational purposes only. For any other purpose, no part of the work may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The work has been developed for automotive applications only. It has neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

Table of Contents

1 Scope of this document

This document specifies requirements on the E2E Protocol. The E2E protocol defines abstract mechanisms to provide End-to-End communication protection according to requirements of ISO26262:2011 [1]. These mechanisms shall allow safe data transmission of safety related data for all integrity levels defined by [1] over a non-safety-related communication path. This document covers the protocol part only and therefore the End-to-End path just partly.

These requirements shall be used as a basis for the specification of detailed E2E mechanisms and their usage in AUTOSAR implementations.

Note: The document contains well known requirements from classic platform documents and brings in new requirements for the adaptive platform as far as foreseen. Use Cases for E2E protection in adaptive platform are under elaboration. More details on the relevant use cases will be added within next version of this document.

This is a draft specification to indicate the intended scope and direction of discussion to the AUTOSAR development community. This specification has seen less quality measures, less discussions among partners and may, generally, be in a less mature state.

2 How to read this document

2.1 Conventions to be used

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template, chapter Support for Traceability ([2]).

The verbal forms for the expression of obligation specified in [TPS_STDT_00053] shall be used to indicate requirements, see Standardization Template, chapter Support for Traceability ([2]).

3 Acronyms and Abbreviations

The glossary below includes acronyms and abbreviations relevant to AUTOSAR_RS_E2E that are not included in the AUTOSAR glossary [3].

Acronym / Abbreviation:	Description:
E2E	End-to-End.
E2E Profile	A set of combined E2E measures as efficient solution for a particular communication stack.
BER	Bit Error Rate - a rate of corrupted bits in a byte stream, e.g. 1e-5.

Table 3.1: Acronyms and Abbreviations

4 Functional Overview

Safety-related automotive systems often use a safe data transmission to protect communication between components (as required by ISO 26262:2011 [1]), 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 (cf. diagnostic coverage, safe failure fraction) and that the rate of undetected dangerous errors is below some allowed limit (cf. residual error rate, probability of dangerous failure per hour or probability of dangerous failure on demand).

4.1 Functional safety and communication

With respect to the exchange of information in safety-related systems, the mechanisms for the in-time detection of causes for faults, or effects of faults as listed below, can be used to design suitable safety concepts, e.g. to achieve freedom from interference between system elements sharing a common communication infrastructure (see ISO 26262-6:2011, annex D.2.4).

4.1.1 Repetition of information

A type of communication fault, where information is received more than once.

4.1.2 Loss of information

A type of communication fault, where information or parts of information are removed from a stream of transmitted information.

4.1.3 Delay of information

A type of communication fault, where information is received later than expected.

4.1.4 Insertion of information

A type of communication fault, where additional information is inserted into a stream of transmitted information.

4.1.5 Masquerading

A type of communication fault, where non-authentic information is accepted as authentic information by a receiver.

4.1.6 Incorrect addressing

A type of communication fault, where information is accepted from an incorrect sender or by an incorrect receiver.

4.1.7 Incorrect sequence of information

A type of communication fault, which modifies the sequence of the information in a stream of transmitted information.

4.1.8 Corruption of information

A type of communication fault, which changes information.

4.1.9 Asymmetric information sent from a sender to multiple receivers

A type of communication fault, where receivers do receive different information from the same sender.

4.1.10 Information from a sender received by only a subset of the receivers

A type of communication fault, where some receivers do not receive the information.

4.1.11 Blocking access to a communication channel

A type of communication fault, where the access to a communication channel is blocked.

4.2 Sources of faults in E2E communication

E2E communication protection aims to detect and mitigate the causes for or effects of communication faults arising from:

1. (systematic) software faults,
2. (random) hardware faults,
3. transient faults due to external influences.

These three sources are described in the sections below.

4.2.1 Software faults

Software like, communication stack modules and RTE, may contain faults, which are of a systematic nature. Systematic faults may occur in any stage of the system's life cycle including specification, design, manufacturing, operation, and maintenance, and they will always appear when the circumstances (e.g. trigger conditions for the root-cause) are the same. The consequences of software faults can be failures of the communication, like interruption of sending of data, overrun of the receiver (e.g. buffer overflow), or underrun of the sender (e.g. buffer empty). To prevent (or to handle) resulting failures the appropriate technical measures to detect and handle such faults (e.g. program flow monitoring or E2E supervision) have to be considered.

4.2.2 Random hardware faults

A random hardware fault is typically the result of electrical overload, degradation, aging or exposure to external influences (e.g. environmental stress) of hardware parts. A random hardware fault cannot be avoided completely, but its probability can be evaluated and appropriate technical measures can be implemented (e.g. diagnostics).

4.2.3 External influences, environmental stress

This includes influences like EMI, ESD, humidity, corrosion, temperature or mechanical stress (e.g. vibration).

4.3 Safe End-to-End communication in AUTOSAR

To provide a safe End-to-End communication, a solution shall be integrated within the AUTOSAR methodology which does require no or a minimal amount of additional non-standard code like wrappers.

The functionality of End-to-End communication protection is to be supported by the E2E Protocol.

The E2E protocol provides

- mechanisms to detect a subset of communication faults listed in 4.1. The relevant communication faults depend on the type of communication (e.g. periodic, non-periodic, sender/receiver, etc.).
- the definition of profiles 1, 2, 4, 5, 6, 7, 11 and 22 including check and protect functions for one single data transfer. The appropriate profile is to be selected according to the used physical bus layer and the size of the transferred data.
- an optional state machine describing the logical algorithm of E2E monitoring and state handling for a number of data transfers between two dedicated communication partners independent of the used profile.

Note: Additional architectural measures may be necessary to ensure safe operation of the E2E protocol implementation.

5 Requirements tracing

The following table references the features and links to the fulfillments of these.

Feature	Description	Satisfied by
[RS_Main_00010]	AUTOSAR shall support the development of safety related systems	[RS_E2E_08527] [RS_E2E_08528] [RS_E2E_08529] [RS_E2E_08530] [RS_E2E_08533] [RS_E2E_08534] [RS_E2E_08539] [RS_E2E_08540] [RS_E2E_08541] [RS_E2E_08542] [RS_E2E_08543] [RS_E2E_08544] [RS_E2E_08545] [RS_E2E_08546] [RS_E2E_08547] [RS_E2E_08548]
[RS_Main_01002]	AUTOSAR shall support service-oriented communication	[RS_E2E_08540] [RS_E2E_08541]
[RS_Main_01003]	AUTOSAR shall support data-oriented communication	[RS_E2E_08540] [RS_E2E_08541]

Table 5.1: Requirements traceability

6 Requirements Specification

6.1 Functional Requirements

6.1.1 Supported communication models and features

E2E protocol is defined to support different types of message-based communication. Signal-based communication:

- periodic/ mixed periodic sender receiver communication

Service-oriented communication:

- periodic/mixed periodic event-based communication
- non-periodic method-based communication (client/server communication)

[RS_E2E_08540] E2E protocol shall support protected periodic/mixed periodic communication ⌈

Type:	draft
Description:	The E2E Protocol shall support protected periodic communication. This includes the following periodicity: • periodic • mixed-periodic
Rationale:	E2E mechanism for message-oriented communication
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	• Sender-receiver communication in CP (e.g. the following use cases – Receiver being invoked independently from Sender – Receiver being invoked on arrival of data – Mixed: Receiver being invoked when data arrives and independently.) • Events implement message-oriented communication in AP service interfaces.
Supporting Material:	–

⌋*(RS_Main_00010, RS_Main_01002, RS_Main_01003)*

[RS_E2E_08541] E2E protocol shall support protected non-periodic communication ⌈

Type:	draft
Description:	This E2E Protocol shall support protected non-periodic communication. The following shall be supported: • Synchronous call (client gets activated when the return is available)
Rationale:	E2E mechanism for service-oriented communication
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Service-oriented client-server communication via SOME/IP methods.
Supporting Material:	–

⌋*(RS_Main_00010, RS_Main_01002, RS_Main_01003)*

[RS_E2E_08542] E2E protocol shall support dynamic restart of communication peers ⌈

Type:	draft
Description:	E2E Protocol shall support: • dynamic restart of communication peers and their late start • different message frequencies/cycles at receiver and sender (over/undersampling) • multiple receivers with different message cycles.
Rationale:	Depending on the variance in startup behavior and expected message frequency of the communication partners a later start or over/undersampling needs to be handled by the protection mechansim.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Communication between applications of main chassis ECU and power steering ECU to prevent an erroneous steering intervention due to a corruption of the transmitted data.
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08543] E2E protocol shall support static and dynamic length of transmitted data ⌈

Type:	draft
Description:	E2E Protocol shall support both static and dynamic length of transmitted data.
Rationale:	Depending on the used protocol static or dynamic length of transmitted data needs to be handled by the protection mechanism.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	E2E protected transmission of a variable length array over SOME/IP.
Supporting Material:	–

⌋*(RS_Main_00010)*

6.1.2 E2E detected faults

E2E protocol is defined to cover a number of faults described in 4.1. However, it depends on the type of communication which kind of faults can be detected, e.g. for non-periodic event-based communication loss of communication data cannot be detected by E2E protocol mechanisms.

[RS_E2E_08544] E2E protocol shall provide a timeout detection mechanism ⌈

Type:	draft
Description:	E2E Protocol shall provide a configurable mechanism to detect timeouts and delayed data.
Rationale:	This mechanism can be used to detect loss and delay of communication data, as requested by ISO 26262.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	• Detection of lost or delayed messages in periodic sender/receiver communication • Detection of lost or delayed events in periodic service-oriented communication • Detection of lost or delayed method responses in non-periodic method communication
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08545] E2E protocol shall provide a detection mechanism for corrupted data ⌈

Type:	draft
Description:	E2E protocol shall provide a detection mechanism for corrupted data
Rationale:	This mechanism can be used to detect corrupted communication data, as requested by ISO 26262.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	• Detection of corrupted messages in sender/receiver communication • Detection of corrupted messages in periodic event-based communication • Detection of corrupted method requests/responses in non- periodic method requests
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08546] E2E protocol shall provide a detection mechanism for masquerade or incorrect addressing ⌈

Type:	draft
Description:	E2E protocol shall provide a detection mechanism for masquerading or incorrect addressing
Rationale:	This mechanism can be used to detect masquerade or incorrect addressing of communication data, as requested by ISO 26262.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	• Detection of masquerading or incorrect addressed data in sender/receiver communication • Detection of masquerading or incorrect addressed data in periodic event-based communication • Detection of masquerading or incorrect addressed data in non- periodic method request/responses
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08547] E2E protocol shall provide a detection mechanism for repetition, insertion or incorrect sequence of data ⌈

Type:	draft
Description:	E2E protocol shall provide a detection mechanism for repetition, insertion or incorrect sequence of data
Rationale:	This mechanism can be used to detect repeated, inserted communication data or data with incorrect sequence, as requested by ISO 26262.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	• Detection of repeated, inserted messages or incorrect sequence of messages in sender/receiver communication • Detection of repeated, inserted messages or incorrect sequence of messages in periodic event-based communication • Detection of repeated method responses in non-periodic method requests
Supporting Material:	–

⌋*(RS_Main_00010)*

6.1.3 E2E Algorithms and Profiles

E2E protocol is defined to cover various sizes of exchanged data and different types of physical bus medium. Therefore, a number of E2E profiles are created. Each E2E profile provides a set of E2E measures as required in 6.1.2.

[RS_E2E_08528] E2E protocol shall provide different E2E profiles ⌈

Type:	draft
Description:	E2E Protocol shall provide E2E profiles, where each E2E profile completely defines a particular safety protocol (including header structure, behavior as state machine, error handling etc). Each E2E profile shall be an efficient solution for a particular communication stack used underneath (which are either FlexRay, CAN, CAN FD, LIN or Ethernet), used data length and data frequency, and the required integrity level (see [1]) of the exchanged data. Note: Each communication stack (e.g. FlexRay) has different BER, 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 The profiles are supposed to cover typical combinations of above factors.
Rationale:	Interoperability of safety-related communication partners, usage of QM communication system.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	- E2E profile with 8-bit CRC for CAN/CAN FD - E2E profile with 16-bit CRC for long FlexRay signals, - E2E profile with 32/64-bit CRC for Ethernet.
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08530] Each E2E profile shall have a unique Profile ID, define precisely a set of mechanisms and its behavior in a semi-formal way ⌈

Type:	draft
Description:	Each E2Eprofile defined within the library shall: - Have a unique Profile ID. - Define precisely a set of mechanisms (e.g. CRC of a particular polynomial). - Define its behavior in a semi-formal way (including state machines, error handling etc).
Rationale:	A profile 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.
Dependencies:	–
AppliesTo:	AP, CP
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 Profile than ECU2.
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08529] Each E2E profile shall use an appropriate subset of specific protection mechanisms ⌈

Type:	draft
Description:	Each of the defined E2E profiles shall use an appropriate subset of the following mechanisms: • Sequence number (different sizes possible; in the state-of-art it is alternatively called alive counter or consecutive number) • CRC with different Bit length • IDs: Source ID, Destination ID, Data ID • Timeout • Length 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 checksum.
Rationale:	These are typical mechanisms used by safety protocols, and they can be realized by AUTOSAR.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Mechanisms used in an exemplary profile: 4-bit sequence counter, CRC8, Data ID, timeout.
Supporting Material:	–

⌋(*RS_Main_00010*)

[RS_E2E_08533] CRC used in a E2E profile shall be different than the CRC used by the underlying physical communication protocol ⌈

Type:	draft
Description:	CRC used in each E2E profile shall be different than the CRC used by the underlying communication protocols (FlexRay, CAN, CAN FD, LIN, Ethernet), 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.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	If profile X is supposed to be used only for FlexRay, then its CRC shall be different than the one of FlexRay.
Supporting Material:	–

⌋(*RS_Main_00010*)

[RS_E2E_08534] E2E Protocol shall provide E2E Check status to the application ⌈

Type:	draft
Description:	E2E Protocol shall provide E2E status of a single checked data to the application layer.
Rationale:	Error handling strategies are “application dependent”, and cannot be “a priori defined”.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Enable error-dependent reaction of the application using E2E Protocol.
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08548] E2E Protocol shall provide E2E overall state to the application ⌈

Type:	draft
Description:	E2E Protocol shall optionally provide E2E overall state of the so far checked data to the application layer.
Rationale:	Error handling strategies are “application dependent”, and cannot be “a priori defined”.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Enable error-dependent reaction of the application using E2E Protocol.
Supporting Material:	–

⌋*(RS_Main_00010)*

[RS_E2E_08539] An E2E protection mechanism for inter-ECU communication of short to large data shall be provided ⌈

Type:	draft
Description:	The E2E protocol shall support protection of short (ex. 8 bytes) and large (ex. 4KB, up to 4MB, as application requires), composite data with dynamic-length over TCP/IP and over LIN/CAN/CAN TP/CAN FD/FlexRay/Ethernet. Note: The max length of protected data depends on the architecture and needs to be evaluated by quantitative analysis within the project using the E2E protocol profile.

▽

△

Rationale:	Large, composite data need specific protection mechanisms.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Communication between applications of main chassis ECU and power steering ECU. (to be detailed)
Supporting Material:	–

⌋(*RS_Main_00010*)

6.2 Safety applicability and overall safety assumptions

[RS_E2E_08527] E2E protocol shall be designed to fulfill ISO 26262 ⌈

Type:	draft
Description:	The E2E protocol shall provide error detection for communicating safety related data according to ISO 26262 [1].
Rationale:	E2E communication protection is state-of-art in automotive safety-related series products.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Communication between applications of main chassis ECU and power steering ECU.
Supporting Material:	–

⌋(*RS_Main_00010*)

7 References

[1] ISO 26262 (Part 1-10) – Road vehicles – Functional Safety, First edition
http://www.iso.org

[2] System Template
AUTOSAR_TPS_SystemTemplate

[3] Glossary
AUTOSAR_TR_Glossary