Document Title	Requirements on E2E for Adaptive Platform
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	847

Document Status	Final
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	17-03

Document Change History			
Date	**Release**	**Changed by**	**Description**
2017-03-31	17-03	AUTOSAR Release Management	• Initial release

Disclaimer

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_AdaptiveE2E 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).

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

- 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 and state handling 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 specified in [4] 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_Main_01002]	AUTOSAR shall support service-oriented communication	[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

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

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

⌋*(RS_Main_00010, RS_Main_01003)*

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

Type:	draft
Description:	This E2E mechanism 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:	–
Applies to:	AP
Use Case:	Service oriented/client-server communication as used in AP architectures (to be detailed). Methods implement client-server communication in AP service interfaces.
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:	
Dependencies:	–
Applies to:	AP
Use Case:	(to be detailed)
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:	–
Applies to:	AP
Use Case:	E2E protected transmission of a variable length array over SOME/IP.
Supporting Material:	–

⌋(*RS_Main_00010*)

6.1.2 E2E Algorithms and Profiles

[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 commmunication system.
Dependencies:	–
Applies to:	AP
Use Case:	Profile with 8-bit CRC for CAN, and 16-bit CRC for long FlexRay signals, 32/64-bit CRC for Ethernet.
Supporting Material:	–

⌋(*RS_Main_00010*)

[RS_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:	draft
Description:	Each E2Eprofile defined within the library shall: • Have a unique 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:	–
Applies to:	AP
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 of the defined E2E profiles 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:	–
Applies to:	AP
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:	–
Applies to:	AP
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 error information for the detected communication failure ⌈

Type:	draft
Description:	E2E Protocol shall provide to the application layer the error information about the detected communication failure.
Rationale:	Error handling strategies are “application dependent”, and cannot be “a priori defined”.
Dependencies:	–
Applies to:	AP
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:	This E2E mechanism shall support protection of short (8 bytes) up to large (4kB), composite data with dynamic-length over TCP/IP and over LIN/CAN/CANTP/FlexRay/Ethernet.
Rationale:	Large, composite data need specific protection mechanisms.
Dependencies:	–
Applies to:	AP
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 protocols shall be applicable up to ASIL D ⌈

Type:	draft
Description:	The protocols shall provide the error detection that is sufficient for transmitting safety-related data for all integrity levels defined in [1], through a communication stack implemented as QM software.
Rationale:	E2E communication protection is state-of-art in automotive safety-related series products.
Dependencies:	–

Applies to:	AP
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

[4] Requirements on AUTOSAR Features
AUTOSAR_RS_Features