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

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R25-11

Document Change History

Date	Release	Changed by	Description
2025-11-27	R25-11	AUTOSAR Release Management	• Editorial changes
2024-11-27	R24-11	AUTOSAR Release Management	• E2E timeout detection rephrased
2023-11-23	R23-11	AUTOSAR Release Management	• Editorial changes
2022-11-24	R22-11	AUTOSAR Release Management	• Editorial changes
2021-11-25	R21-11	AUTOSAR Release Management	• No content changes
2020-11-30	R20-11	AUTOSAR Release Management	• No content changes
2019-11-28	R19-11	AUTOSAR Release Management	• Functional requirements: information added • Requirements moved from CP SRS E2E • Changed Document Status from Final to published

▽

△

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 ISO 26262:2018 (all parts) [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

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see [2, Standardization Template].

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

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 26262:2018 (all parts) [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
    - the rate of undetected dangerous errors shall be 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 26262-6:2018, annex D.2.4).

Type of communication fault	Description
Repetition of information	A type of communication fault, where information is received more than once.
Loss of information	A type of communication fault, where information or parts of information are removed from a stream of transmitted information.
Delay of information	A type of communication fault, where information is received later than expected.
Insertion of information	A type of communication fault, where additional information is inserted into a stream of transmitted information.
Masquerading	A type of communication fault, where non-authentic information is accepted as authentic information by a receiver.
Incorrect addressing	A type of communication fault, where information is accepted from an incorrect sender or by an incorrect receiver.
Incorrect sequence of information	A type of communication fault, which modifies the sequence of the information in a stream of transmitted information.
Corruption of information	A type of communication fault, which changes information.
Asymmetric information sent from a sender to multiple receivers	A type of communication fault, where receivers do receive different information from the same sender.
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.
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. Software faults,
2. Random hardware faults,
3. Transient faults

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 Transient faults

Transient faults typically result from external influences or 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.

4.3.1 E2E protection concepts

An E2E protection concept is more than just adding adequate safety mechanisms to data elements (e.g. using E2E Profile 1 or 2). To ensure the integrity of a communication channel with the required safety integrity level acc. to ISO 26262 the E2E protection concept needs to consider the safety-related properties of the data transmitted via a bus network that requires protection. Basic principles to implement an E2E protection concept that focuses on correctness, consistency, completeness, timeliness and the detection of non-availability of data are provided in this chapter.

Note: For an E2E protection concept that focuses on ensuring the availability of data, an implementation of the communication channel with a sufficient fault tolerance is needed (e.g. using independent redundant channels).

Note: The usage of redundant communication channels may create a need for additional safety mechanisms (e.g. to ensure the consistency of the data streams when transmitted independently).

Typical basic principles for effective E2E protection concepts are[1]:

1. The infrastructure used for data transmission (e.g. Buses, Gateways, etc.) is designed and implemented in such way that it cannot systematically interfere with the used E2E protection (e.g. by unpacking and changing protected data).

2. In case of an internal fault during provision of data,

   - the provider (e.g. sender or client) ensures that it sends out either data explicitly labeled as invalid (i.e. only the specific data elements that are possibly affected by this internal fault) or else no data (i.e. fail-safe respectively fail-silent behavior of sender in case of a severe fault).

3. In normal operation mode,

   - the provider (e.g. sender or client) of the data

     - groups the data as pre- determined (e.g. to ensure consistency for a set of data) and protects the grouped data with suitable protection mechanisms prior to their transmission.

     - ensures that it sends out valid data, only.
       In this context valid data means:

       - Data fully complying with their required safety-related properties

       - Data complying with their required safety-related properties to the extent signaled by an additionally provided qualifier (i.e. signal qualifier)

       - Data explicitly labeled as invalid data (e.g. using a signal invalid value)

     - ensures in case of periodic/ mixed periodic communication that it sends out valid data on a regular basis (e.g. cyclic).

   - the consumer (e.g. receiver, client or server) of the data

     - monitors whether new data has arrived on a regular basis (e.g. cyclic) independently from an external trigger condition coming from elements to which it wants to achieve freedom from interference (e.g. communication stack).

     - is able to detect relevant communication faults within its determined time interval by evaluating the protection mechanisms of the received data and in case of periodic/ mixed periodic communication its internal timeout monitoring.

4. In case a communication fault is detected

[1] These aspects are described based for a sender/receiver type of communication but apply more or less in same sense to other types of communication.

  - the consumer of the protected data (e.g. receiver, client or server) autonomously initiates the necessary reactions to mitigate the detected communication fault within its determined time interval in compliance with the functional safety concept of the system (i.e. fail-safe respectively fail-silent behavior of receiver).

5. Based on the ISO26262 the fault tolerance time interval (FTTI) of the respective safety-related system is the allowed time interval for fault detection and mitigation including the relevant data exchange part and the corresponding communication path.

    - The fault tolerance time interval concerning the whole system (absolute FTTI), the allowed time interval includes the allowed time interval for the detection and mitigation of faults at the provider of the date (e.g. sender), the time interval required for robustness of data transmission during normal operation (e.g. to compensate gateways) and the allowed time interval for the detection and mitigation of faults at the consumer of the data (e.g. receiver).

    - The fault tolerance time interval concerning the data exchange part and the corresponding communication path only (relative FTTI), corresponds to the maximum tolerated duration of erroneous data, and is thus the allowed time interval for the detection and mitigation of faults at the consumer of the data (e.g. receiver).

4.3.2 Integrity of a communication channel

To determine the integrity of communication and to distinguish if the received data are valid the consumer of the data (e.g. receiver) can:

- evaluate each received protected message separately and
- monitor all evaluation results of a number of protected data received within a determined time interval for error detection and qualification t_{EDQ} up to the data received at last.

To implement the monitoring function the consumer of the protected data (e.g. receiver) creates a history of the received data. Valid received data are stored with a history as follows:

- Generation 0 is the latest (up to date) received valid data
- Generation 1 is the second-latest received valid data
- Generation 2 is the third-latest received valid data
- etc.

To do so, each recently received valid message is stored as Generation 0 having a reference value indicating its age set to 0. Every time the consumer of the protected data (e.g. receiver) checks for reception of new data it increments the age of its already received data by 1. Stored data can be used as basis for a safety related functionality provided by the consumer of the protected data (e.g. receiver) as long as its age reference value is less a determined boundary value N. The parameter N can be derived by dividing the determined time interval for error detection and qualification t_{EDQ} with the cycle time used for its regular transmission (e.g. for a receiver having a t_{EDQ} = 160ms and a regular cycle time of 20ms the value N = 160ms/20ms = 8).

In case that sufficiently up to date data is no longer available, the consumer's (e.g. receiver's) application applies a safe reaction determined in the safety concept. Such reaction can be a degraded mode.

5 Requirements tracing

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

Requirement	Description	Satisfied by
[RS_SAF_31301]	E2E Protection with E2E Transformer and E2E Library	[RS_E2E_08538] [RS_E2E_08544] [RS_E2E_08545] [RS_E2E_08546] [RS_E2E_08547]
[RS_SAF_31302]	Allow integrators to configure safety mechanisms to detect communication faults	[RS_E2E_08528] [RS_E2E_08539] [RS_E2E_08543]

Table 5.1: Requirements Tracing

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 ⌈

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_E2E_08541] E2E protocol shall support protected non-periodic communication ⌈

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) • Decision making for applying the method call on server side based on E2E results
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_E2E_08542] E2E protocol shall support dynamic restart of communication peers ⌈

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 mechanism.
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_E2E_08543] E2E protocol shall support variable length of transmitted data

Upstream requirements: RS_SAF_31302

⌈

Description:	E2E protocol shall support variable 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:	–

⌋

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

Upstream requirements: RS_SAF_31301

⌈

Description:	E2E protocol shall provide a configurable mechanism to detect timeouts and delayed data during periodic communication.
Rationale:	This mechanism can be used to detect loss and delay of communication data, as requested by ISO 26262-6:2018 [1], annex D.2.4.
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
Supporting Material:	–

⌋

Note: A timeout detection mechanism to identify lost or delayed method responses in non-periodic method communication cannot be provided by an E2E protocol specification. This kind of mechanism has to be specified and implemented either by the application itself or as part of communication management functionality.

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

Upstream requirements: RS_SAF_31301

⌈

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 26262-6:2018 [1], annex D.2.4.
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_E2E_08546] E2E protocol shall provide a detection mechanism for masquerade or incorrect addressing

Upstream requirements: RS_SAF_31301

⌈

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 26262-6:2018 [1], annex D.2.4.
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_E2E_08547] E2E protocol shall provide a detection mechanism for repetition, insertion or incorrect sequence of data

Upstream requirements: RS_SAF_31301

⌈

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 26262-6:2018 [1], annex D.2.4.
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:	–

⌋

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

Upstream requirements: RS_SAF_31302

⌈

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 depends 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_E2E_08530] Each E2E profile shall define a set of protection mechanisms and its behavior ⌈

Description:	Each E2E profile defined shall: • 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.). Note: For CP the E2E profiles are provided within the E2E library.

▽

△

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 behavior is needed to achieve interoperability. Mechanisms are to be defined to detect the communication faults described in ISO 26262-6:2018 [1], annex D.2.4.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	Usually one state machine per profile per communicating partner (sender, receiver, client or server) is sufficient. ECU1 and ECU2 communicating. ECU1 has different implementation of E2E profile than ECU2.
Supporting Material:	–

⌋

[RS_E2E_08549] Each E2E profile shall have a unique Profile ID ⌈

Description:	Each E2E profile shall have a unique Profile ID.
Rationale:	It needs to be ensured that provider and consumer use the same E2E profile.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	E2E protected communication
Supporting Material:	–

⌋

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

Description:	Each of the defined E2E profiles shall use an appropriate subset of the following mechanisms: • Sequence counter with different sizes (alternatively used as alive counter) • 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 counter and IDs, if used, should be all part of the transmitted data element. However, it is allowed that in a given profile, the sequence counter and/or IDs are “hidden” (not transmitted), but included in the checksum.
Rationale:	These are typical mechanisms used for communication protection, 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_E2E_08533] CRC used in a E2E profile shall be different than the CRC used by the underlying physical communication protocol ⌈

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_E2E_08534] E2E protocol shall provide E2E Check status to the application ⌈

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_E2E_08548] E2E protocol shall provide E2E overall state to the application ⌈

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_E2E_08539] An E2E protection mechanism for inter-ECU communication of short to large data shall be provided

Upstream requirements: RS_SAF_31302

⌈

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.
Supporting Material:	–

⌋

[RS_E2E_08550] The implementation of the E2E Supervision shall provide at least one of the E2E Profiles ⌈

Description:	The implementation of the E2E Supervision shall provide at least one of the E2E Profiles.
Rationale:	Implementation of the Protocol requires at least one profile, otherwise the state machine would not work.
Dependencies:	–
AppliesTo:	AP, CP
Use Case:	E2E requires at least one profile to supervise a communication.
Supporting Material:	–

⌋

6.2 Safety applicability and overall safety assumptions

[RS_E2E_08527] Implementation of E2E protocol shall fulfill ISO 26262 ⌈

Description:	The E2E protocol shall be implemented 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:	–

⌋

6.3 E2E Transformer

The 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.

[RS_E2E_08538] An E2E Transformer shall be provided

Upstream requirements: RS_SAF_31301

⌈

Description:	An 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.
Dependencies:	–
AppliesTo:	CP
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
Supporting Material:	–

⌋

6.4 E2E Library

The E2E Library provides a set of safety protocols, in a form of library functions invoked by SW-Cs. It provides:

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

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.

[RS_E2E_08531] E2E Library shall call the CRC routines of CRC library ⌈

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
Dependencies:	–
AppliesTo:	CP
Use Case:	CRC8 of CRC library to be used in one of the profiles for protecting CAN communication.
Supporting Material:	–

⌋

[RS_E2E_08537] SW-Cs shall tolerate a number of invalid/corrupted received data elements

Upstream requirements:

⌈

Description:	SW-Cs shall tolerate a number of data elements that are invalid/corrupted but not detected by E2E as defined in architecture specific safety analysis for the used E2E protocol.

▽

△

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) and suitability of applied E2E profile. Allowing at least one invalid signal (in a sequence of received signals) that is not detected by E2E mechanisms enables for instance the usage of profiles that contain shorter CRCs like E2E profiles 01, 11 and 02, 22.
Dependencies:	–
AppliesTo:	AP, CP
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 faults or SW faults in E2E Library causing that CRC Sequence Counter computation does not detect an error.
Supporting Material:	–

⌋

7 Moved Requirements

The following requirements were moved from the document Requirements on E2E Communication Protection (UID 651, SRS) with release R19-11 of AUTOSAR Classic Platform and Foundation. Please find a mapping between old and new requirement IDs in the table below.

Old requirement ID	New requirement ID
SRS_E2E_08540	[RS_E2E_08540]
SRS_E2E_08538	[RS_E2E_08538]
SRS_E2E_08528	[RS_E2E_08528]
SRS_E2E_08527	[RS_E2E_08527]
SRS_E2E_08529	[RS_E2E_08529]
SRS_E2E_08530	[RS_E2E_08530]
SRS_E2E_08531	[RS_E2E_08531]
SRS_E2E_08533	[RS_E2E_08533]
SRS_E2E_08534	[RS_E2E_08534]
SRS_E2E_08536	RS_E2E_08536
SRS_E2E_08537	[RS_E2E_08537]
SRS_E2E_08539	[RS_E2E_08539]

Table 7.1: Mapping of moved requirements

8 References

[1] ISO 26262:2018 Road vehicles -– Functional Safety
https://www.iso.org

[2] Standardization Template
AUTOSAR_FO_TPS_StandardizationTemplate

[3] Glossary
AUTOSAR_FO_TR_Glossary

A Changehistory of AUTOSAR traceable items

A.1 Traceable item history of this document according to AUTOSAR Release R25-11

A.1.1 Added Requirements in R25-11

none

A.1.2 Changed Requirements in R25-11

[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_E2E_08549]

A.1.3 Deleted Requirements in R25-11

none

A.2 Traceable item history of this document according to AUTOSAR Release R24-11

A.2.1 Added Requirements in R24-11

none

A.2.2 Changed Requirements in R24-11

[RS_E2E_08544]

A.2.3 Deleted Requirements in R24-11

none