Document Title	Requirements on Intrusion Detection System
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	976

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R23-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2023-11-23	R23-11	AUTOSAR Release Management	• No content changes
2022-11-24	R22-11	AUTOSAR Release Management	• No content changes
2021-11-25	R21-11	AUTOSAR Release Management	• no content change
2020-11-30	R20-11	AUTOSAR Release Management	• Initial release

Disclaimer

Contents

1 Scope of Document

This document specifies requirements for the AUTOSAR **Intrusion Detection System** (**IDS**) . The following section gives an overview of the elements of the IDS and in which AUTOSAR document the element is described.

1.1 General Architecture of a distributed onboard IDS

An onboard IDS according to the AUTOSAR standard consists of the following elements:

- Security Sensors
- Intrusion Detection System Manager (IdsM)
- Security Event Memory (Sem)
- Intrusion Detection System Reporter (IdsR)

Figure 1.1 shows the principle architecture of the distributed onboard IDS.

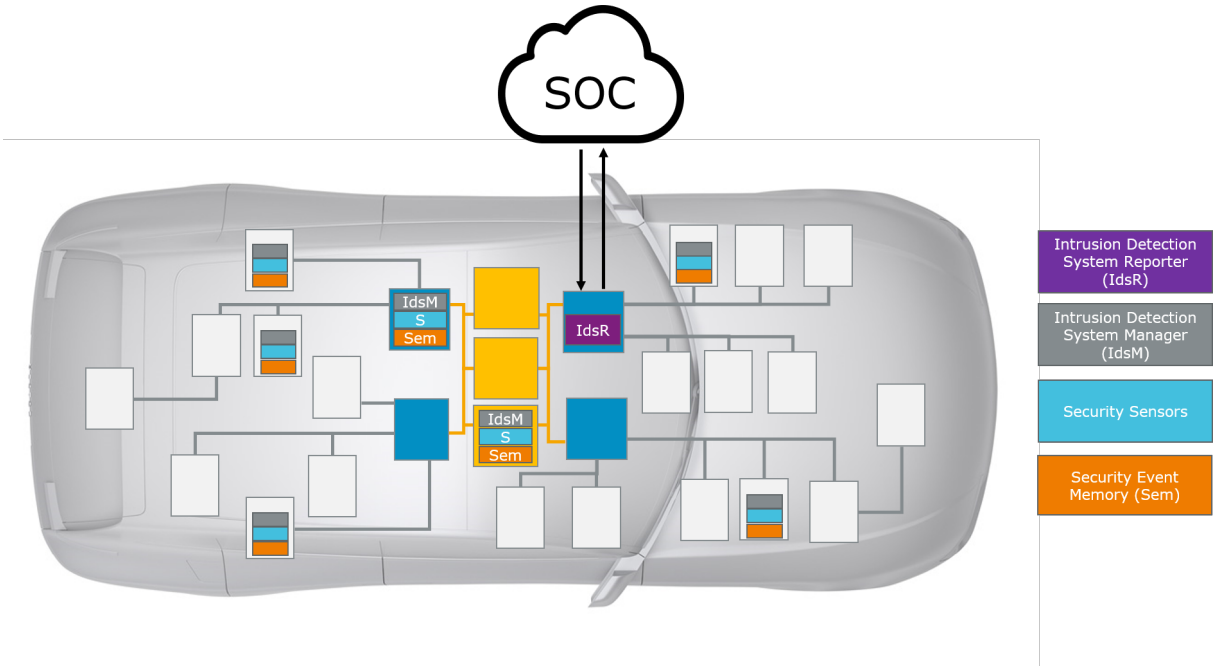

Figure 1.1: Architecture of a distributed onboard IDS

The elements of the onboard IDS are briefly described in the following sections.

1.2 Security Sensors and Security Events

AUTOSAR BSW modules, CDD and SWC can act as **Security Sensors**. Security sensors report **Security Events** (**SEv**) to the IdsM. AUTOSAR standardizes a subset of **Security Event Types** which can be reported by the AUTOSAR BSW. Each BSW SWS lists the **Security Event Types** which are reported by the respective module as described in SWS BSW General [1].
An overview of the **Security Event Types** which are standardized by AUTOSAR is available via the General Definition Security Events [2].

SWC and CDD can also report custom **Security Event Types** which are not standardized in AUTOSAR. The properties of **Security Event Types** which are reported by specific ECUs can be specified by using the **Security Extract** (**SecXT**) [3] .

1.3 Intrusion Detection System Manager

The **IdsM** buffers the reported security events. Furthermore the IdsM applies a set of consecutive filters to the reported SEv. A set of consecutive filters is called a **Filter Chain**. If SEv pass their Filter Chain they are regarded as **Qualified Security Events** (**QSEv**).
Depending on the configuration the IdsM can

- pass the QSEv to a **Security Event Memory** (**Sem**) to persist it on the local ECU.
- and/or serialize the QSEv and transmit it to the IdsR.

In this document the system requirements of the IdsM are specified. The SWS IdsM CP [4] specifies the software requirements for the Classic Platform IdsM. The SWS IdsM AP [5] specifies the software requirements for the Adaptive Platform IdsM.

1.4 Intrusion Detection System Reporter

The **Intrusion Detection System Reporter** (**IdsR**) receives the QSEv from the IdsM instances of the different ECUs. The communication protocol between the IdsM instances and the IdsR is specified in the IdsM protocol specification [6]. The IdsR should typically further enrich the received data e.g. with geo-position. Depending on the needs of the OEM the data can be propagated to a **SOC** for further analysis in a **SIEM** solution. A specification of the IdsR is not provided by AUTOSAR.

2 Conventions to be used

2.1 Document Conventions

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template, chapter Support for Traceability ([7]).

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 ([7]).

3 Acronyms and abbreviations

3.1 Acronyms

Acronym	Description:
Filter Chain	A set of consecutive filters which is applied to Security Events-
Intrusion Detection System	An Intrusion Detection System is a security control which detects and processes security events.
Intrusion Detection System Manager	The Intrusion Detection System Manager handles security events reported by security sensors.
Intrusion Detection System Reporter	The Intrusion Detection System Reporter handles qualified security events received from Idsm instances.
Security Extract	The Security Extract specifies which security events are handled by IdsM instances and their configuration parameters.
Security Event Type	A security event type can be identified by its security event type ID. Instances of security event types are called security events and share the same security event type ID.
Security Events	Onboard Security Events are instances of security event types which are reported by BSW or SWC to the IdsM.
Security Event Memory	A user defined diagnostic event memory which is independent from the primary diagnostic event memory.
Security Sensors	BSW or SWC which report security events to the Idsm.
Qualified Security Events	Security events which pass their filter chain are regarded as Qualified Security Events.
Security Incident and Event Management	Process for handling a confirmed security incident
Security Operation Centre	Organization of security and domain experts who are analyzing security events and contributing to mitigation of threats.

Table 3.1: Acronyms

3.2 Abbreviations

Abbreviation	Description:
IDS	Intrusion Detection System
IdsM	Intrusion Detection System Manager
IdsR	Intrusion Detection System Reporter
SecXT	Security Extract
SEv	Security Event
QSEv	Qualified Security Event
Sem	Security Event Memory
SIEM	Security Incident and Event Management
SOC	Security Operation Centre

Table 3.2: Abbreviations

4 Requirements Specification

The following use cases drive the requirements for the onboard **IDS**.

- UC1: Collect data about security events (SEv)
- UC2: Filter qualified onboard security events (QSEv) from security event data
- UC3: Locally store QSEv records
- UC4: Forward QSEv to ECU with **SOC** connection
- UC5: Provide access to locally stored QSEv records
- UC6: Re-configure qualification parameters during operation
- UC7: Update IdsM configuration
- UC8: Protect IdsM configuration
- UC9: Protect IdsM data in transit and in rest

The use case IDs are referenced from the following requirements.

Figure 4.1 shows an abstract functional architecture of the IDS. The principal allocation of the functional elements refers to both the CP and AP altough the actual technical architecture differs as outlined in the respective SWS. The figure shows the overall functional elements of the IDS and which functional elements are covered by the IdsM.

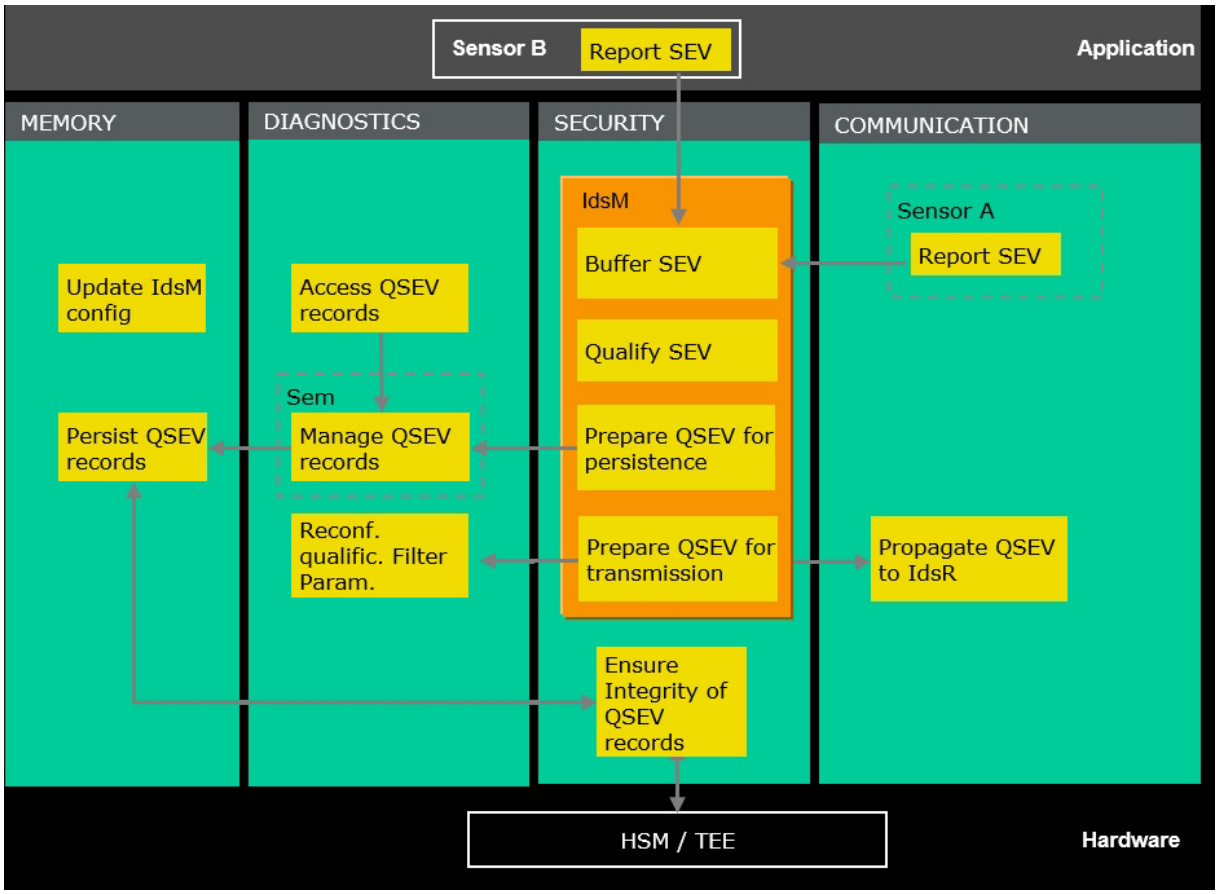

Figure 4.1: Abstract functional elements of the IdsM

4.1 Functional Requirements

4.1.1 Initialization

[RS_Ids_00100]{DRAFT} **Initialization of the IdsM** ⌈

Description:	The IdsM qualification rules shall get initialized at start-up
Rationale:	The IdsM needs configuration information to perform its operation. Therefore, this information shall get recovered from NVM and initialized before it starts its processing operation.
Dependencies:	–
Use Case:	UC8
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.2 Reporting of SEv

[RS_Ids_00200]{DRAFT} **Provide Interface for reporting SEv** ⌈

Description:	The IdsM shall provide interfaces for reporting SEv. The interfaces shall allow to report the following SEv properties: • Security event type: Uniquely identifies the security event type • Context data: Optional data which can be used to analyze the security event in the SOC. • Timestamp: Optional timestamp provided by the sensor. • Count: Optional count provided by the sensor.
Rationale:	Security events can be reported by basic software, complex device drivers and application software to the IdsM.
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.3 Buffering of reported Sev

[RS_Ids_00210]{DRAFT} **IdsM shall buffer reported SEv for callers** ⌈

Description:	The IdsM shall buffer reported SEv for callers
Rationale:	The IdsM shall buffer the SEv and context data for the SEv sensors until the data is completely processed by the IdsM.
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.4 Qualification of SEv

4.1.4.1 Reporting Mode

[RS_Ids_00310]{DRAFT} **Configure reporting mode per Security Event Type and IdsM instance** ⌈

Description:	The IdsM shall support to configure the reporting mode for each **Security Event Type** handled by an IdsM instance. The reporting mode shall include options to (a) turn off processing of SEvs, (b) discard context data, and (c) bypass subsequent filters.
Rationale:	The reporting mode allows to control whether the event is of interest at all and whether it should be further processed.
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

Reporting Mode Level	*Related Behavior*
OFF	IdsM shall discard the SEv without further processing.
BRIEF	If the **SEv** has been reported including context data, IdsM shall shall discard the context data from further processing, transmission, and storage.
DETAILED	If the **SEv** has been reported including context data, IdsM shall keep the context data for potential transmission or persisting of the **QSEv**.
BRIEF_BYPASSING_FILTERS	IdsM shall report or persist the **SEv** without context data without further application of any filter chain.
DE-TAILED_BYPASSING_FILTERS	IdsM shall report or persist the **SEv** with context data (if provided by the sensor) without further application of any filter chain.

Table 4.1: Reporting Mode Filter Values

4.1.4.2 Filter Chains

[RS_Ids_00300]{DRAFT} **Provide configurable filter chains for qualifying SEv** ⌈

Description:	The IdsM shall support the qualification of **SEv** by applying a configurable chain of filters to the reported SEv. One configured sequence of filters is called **Filter Chain**.

▽

△

Rationale:	Not always a single SEv shall be directly handled as a qualified security event. Depending on project specific security analysis one or more filters can be applied to the reported SEv.If an SEv passes all filters of the applied filter chain, the event is qualified (i.e., it is a **QSEv**). The event will then be transmitted and/or persisted.
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

[RS_Ids_00301]{DRAFT} **Provide multiple filter chains** ⌈

Description:	The IdsM shall support the creation of multiple `Filter Chain`s and the individual assignment of each SEv of a given **`Security Event Type`s** to a specific filter chain per IdsM instance.
Rationale:	Different Security Event definitions may require different filter chains.
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.4.3 Machine State Filter

[RS_Ids_00320]{DRAFT} **Support machine state filter** ⌈

Description:	The IdsM shall support the ECU/machine state depended handling of SEvs.
Rationale:	Certain event definitions may be relevant only in certain states and should be ignored in other states.
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.4.4 Sampling Filter

[RS_Ids_00330]{DRAFT} **Support sampling filter** ⌈

Description:	The IdsM shall support the sampling of SEvs.
Rationale:	The data rate for security events that can occur with a very high frequency can be reduced.
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.4.5 Aggregation Filter

[RS_Ids_00340]{DRAFT} **Support Aggregation filter** ⌈

Description:	The IdsM shall support to aggregate multiple SEvs into one QSEv that indicates how often the aggregated SEv occured.
Rationale:	Aggregation of events can reduce resource consumption for SEvs occurring at a high frequency, while maintaining information on the total number of event occurrences.
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.4.6 Threshold Filter

[RS_Ids_00350]{DRAFT} **Support Threshold filter** ⌈

Description:	The IdsM shall support to forward SEvs only, if they occurred more frequently than a configurable threshold within a configurable interval.
Rationale:	SEvs may be triggered on a regular basis by normal operation which should not be reported, however, a deviation from the normal frequency might indicate an incident that should be reported.
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP

▽

△

Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.5 Timestamping of Events

[RS_Ids_00502]{DRAFT} **Event Timestamps** ⌈

Description:	IdsM shall provide mechanisms to add timestamps to SEvs
Rationale:	Analysis of events may require the time of occurrence of events.
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

[RS_Ids_00503]{DRAFT} **Timestamp Sources** ⌈

Description:	IdsM shall provide mechanisms to let application or sensor software provide timestamps.
Rationale:	Project specific applications or sensors may provide more accurate timestamps
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.6 Propagation of QSEv to the IdsR

[RS_Ids_00510]{DRAFT} **The IdsM shall allow to transmit QSEv to the IdsR** ⌈

Description:	IdsM shall allow to transmit the **`QSEv`** and context data by using an IDS protocol [6] which is independent from the underlying bus technology.
Rationale:	QSEv are reported by ECUs which can be connected to the rest of the E/E-Architecture with a variety of bus systems. The **`IdsR`** can relay events to the SOC.
Dependencies:	–
Use Case:	UC4

▽

△

AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.7 Persisting of QSEv

[RS_Ids_00400]{DRAFT} **Persist QSEv records** ⌈

Description:	The IdsM shall be able to locally persist QSEvs via a user defined diagnostic memory. The user defined diagnostic memory shall be separate from the main diagnostic memory to allow separate access control and protection of the NVM block which is used to store the QSEv records. (Such a user defined diagnostic memory is also called a **`Security Event Memory`**) The following properties of a **`QSEv`** shall be persisted: • IDS Protocol header which indicates the protocol version and the used protocol options • Identifier for the instance of the IdsM • Identifier for the instance of the sensor module • Identifier for the SEv which was qualified • Counter which indicates how often the SEv was reported before it was qualified • Time stamp (optional) which indicates the point in time when the SEv was qualified • Context data (optional) which provides additional information which can be evaluated in the an SOC, by a diagnostic tester, or by any other security analysis instance which has access rights. • Signature (optional) which supports IdsM to **`SOC`** integrity and authenticity
Rationale:	Persisted QSEvs can be accessed at a later point in time for analysis without relying on, e.g., network connectivity.
Dependencies:	–
Use Case:	UC3, UC5
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.8 Configuration

[RS_Ids_00600]{DRAFT} **Configuration of SEv** ⌈

Description:	It shall be configurable which SEv are reported to the IdsM.
Rationale:	Depending on a project specific security analysis some **SEv** are regarded as relevant while other SEv are not regarded as relevant. In order to avoid unnecessary calls to the IdsM by the sensor modules this property shall be configurable per security event type per IdsM instance.
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

[RS_Ids_00610]{DRAFT} **Configuration of qualification filters for SEv** ⌈

Description:	It shall be configurable which qualification filters are applied to a SEv by the IdsM
Rationale:	Depending on a project specific security analysis different qualification filters need to be applied to qualify different SEv types.
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

[RS_Ids_00620]{DRAFT} **Configuration of persistency handling for QSEv** ⌈

Description:	It shall be configurable if QSEv shall be locally persisted
Rationale:	Depending on a project specific security analysis and the available ressources (e.g. NVM) decisions about persisting QSEv will be taken. The respective properties (e.g. sizes of buffers) need to be configurable.
Dependencies:	–
Use Case:	UC3
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

[RS_Ids_00630]{DRAFT} **Configuration of propagation handling for QSEv** ⌈

Description:	It shall be configurable if QSEv shall be propagated to a IdsR
Rationale:	Depending on a project specific security analysis and the available resources (e.g. onboard band with) decisions about propagation of QSEv will be taken. The respective properties (e.g. I-PDU for QSEv) need to be configurable.
Dependencies:	–
Use Case:	UC6
AppliesTo:	CP, AP
Supporting Material:	–

⌋*(RS_BRF_02038)*

4.1.9 Re-Configuration

[RS_Ids_00700] Reconfiguration during run-time ⌈

Description:	Support re-configuration of reporting mode during runtime
Rationale:	It shall be possible to change the reporting mode of SEv during runtime. The IdsM shall provide an interface which can be used e.g. by diagnostic routines.
Dependencies:	–
Use Case:	–
AppliesTo:	CP, AP
Supporting Material:	–

⌋*(RS_BRF_02038)*

4.1.10 Update of IdsM Configuration

[RS_Ids_00710] Replacement of complete filter chain configurations ⌈

Description:	The IdsM shall allow to replace complete filter chain configurations.
Rationale:	In situations like end of line programming, ECU initialization in a workshop, or rollout of new updates via OTA it shall be possible to replace complete filter chain configurations
Dependencies:	–
Use Case:	UC7
AppliesTo:	CP, AP
Supporting Material:	The actual replacement/update can be a standard SW update of a logical block performed by FBL or OTA.

⌋*(RS_BRF_02038)*

4.1.11 Security related requirements

4.1.11.1 Basic Software Security Event Types

[RS_Ids_00810] Basic SW security events ⌈

Description:	Basic software modules which are regarded as security relevant, shall report security events to the IdsM.
Rationale:	Whether basic software modules are regarded as security relevant is discussed and decided by a dedicated AUTOSAR working group. Specification of security event types is done based on the needs of the involved AUTOSAR members.
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.11.2 IdsM Security Event Types

[RS_Ids_00820] IdsM Security Events ⌈

Description:	The IdsM shall report IdsM specific security events in the following situations: • If the IdsM traffic limitation was exceeded • If the IdsM context buffers are exhausted • If the IdsM event buffers are exhausted
Rationale:	The IdsM shall provide means to support his own security events
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.11.3 End2End Authenticity of transmitted QSEvs

[RS_Ids_00505]{DRAFT} **Authenticity of QSEvs** ⌈

Description:	IdsM shall support signing QSEvs including all optional data (e.g., context data, timestamp).
Rationale:	Authenticity of events can be ensured.
Dependencies:	–
Use Case:	UC9
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.11.4 Authenticity of stored QSEv records

[RS_Ids_00430]{DRAFT} **Support detection of manipulation of QSEv records** ⌈

Description:	The memory stack shall be able to optionally detect manipulation of persisted QSEv records. If a manipulation of QSEv records was detected, the memory stack shall raise a security event.
Rationale:	Depending on the security analysis of the OEM it may be required to detect manipulation of QSEv records.
Dependencies:	–
Use Case:	UC7
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_BRF_02038*)

4.1.11.5 Availability

[RS_Ids_00511]{DRAFT} **Limit event rate and traffic** ⌈

Description:	IdsM shall support limiting the rate of QSEvs transmitted to the `IdsR` and the bandwidth consumed by these transmissions.
Rationale:	Limit network bus load caused by IDS.
Dependencies:	–
Use Case:	UC9
AppliesTo:	CP, AP

▽

△

Supporting Material:	–

⌋(*RS_BRF_02038*)

4.2 Non-Functional Requirements (Qualities)

No content

5 Requirements Tracing

The following table references the features specified in [8] and links to the fulfillments of these.

Requirement	Description	Satisfied by
[RS_BRF_02038]	AUTOSAR shall support Intrusion Detection System (IDS) security controls	[RS_Ids_00100] [RS_Ids_00200] [RS_Ids_00210] [RS_Ids_00300] [RS_Ids_00301] [RS_Ids_00310] [RS_Ids_00320] [RS_Ids_00330] [RS_Ids_00340] [RS_Ids_00350] [RS_Ids_00400] [RS_Ids_00430] [RS_Ids_00502] [RS_Ids_00503] [RS_Ids_00505] [RS_Ids_00510] [RS_Ids_00511] [RS_Ids_00600] [RS_Ids_00610] [RS_Ids_00620] [RS_Ids_00630] [RS_Ids_00700] [RS_Ids_00710] [RS_Ids_00810] [RS_Ids_00820]

Table 5.1: RequirementsTracing

6 References

[1] General Specification of Basic Software Modules
AUTOSAR_CP_SWS_BSWGeneral

[2] Standardized M1 Models used for the Definition of AUTOSAR
AUTOSAR_FO_MOD_GeneralDefinitions

[3] Security Extract Template
AUTOSAR_FO_TPS_SecurityExtractTemplate

[4] Specification of Intrusion Detection System Manager
AUTOSAR_CP_SWS_IntrusionDetectionSystemManager

[5] Specification of Intrusion Detection System Manager for Adaptive Platform
AUTOSAR_AP_SWS_IntrusionDetectionSystemManager

[6] Specification of Intrusion Detection System Protocol
AUTOSAR_FO_PRS_IntrusionDetectionSystem

[7] Standardization Template
AUTOSAR_FO_TPS_StandardizationTemplate

[8] Requirements on AUTOSAR Features
AUTOSAR_CP_RS_Features

A Change history of AUTOSAR traceable items

Please note that the lists in this chapter also include traceable items that have been removed from the specification in a later version. These items do not appear as hyperlinks in the document.

A.1 Traceable item history of this document according to AUTOSAR Release R23-11

A.1.1 Added Requirements in R23-11

none

A.1.2 Changed Requirements in R23-11

none

A.1.3 Deleted Requirements in R23-11

none