Document Title	Requirements on Security Extract Template
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	979

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R20-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2020-11-30	R20-11	AUTOSAR Release Management	Initial release

Disclaimer

Table of Contents

References

[1] Standardization Template
AUTOSAR_TPS_StandardizationTemplate

1 Introduction

1.1 Scope of this document

This document collects the requirements on the Security Extract Template.

The main purpose of the Security Extract is to define Security Events and their properties as input to the Intrusion Detection System of a vehicle's electronics. The Security Extract can serve as an exchange file to collect the Security Events and their properties from multiple sources during the development process as well as during a maintenance process when vehicles are already in the field.

A Security Extract file is used to configure the Security Events of Intrusion Detection System Manager (IdsM) instances in the ECUs or machines of a vehicle.

It may further be used, for example, as input for a "Security Incident and Event Management" (SIEM) system as part of a "Security Operation Center" (SOC) enabling interpretation of binary data received from the IdsM instances of vehicles.

In short, the key aspects for the usage of the Security Extract are:

- Collect Security Event definitions from multiple sources during development process
- Input to configuration of Security Events for IdsM instances of ECUs and machines of a vehicle
- Input for SIEM systems enabling interpretation of binary data related to Security Events

1.2 Document Conventions

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template, chapter Support for Traceability ([1]).

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 ([1]).

1.3 Guidelines

Existing specifications shall be referenced (in form of a single requirement). Differences to these specifications are specified as additional requirements.

All requirements shall have the following properties:

- Redundancy
  Requirements shall not be repeated within one requirement or in other requirements.
- Clearness
  All requirements shall allow one possibility of interpretation only. Used technical terms that are not in the glossary must be defined.
- Atomicity
  Each Requirement shall only contain one requirement. A Requirement is atomic if it cannot be split up in further requirements.
- Testability
  Requirements shall be testable by analysis, review or test.
- Traceability
  The source and status of a requirement shall be visible at all times.

1.4 Requirements Tracing

Currently no requirements tracing is provided for this document. Requirement tracing will be included in later revision.

2 Requirements

2.1 Requirements related to Security Events

[RS_SECXT_00001] Definition of Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the definition and configuration of Security Events.
Rationale:	It shall be possible to convey events and associated information related to security from a sensor (realized as hardware or software) to a software module that processes these events and the associated information.
Use Case:	Report a Security Event
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00023] Definition of Security Sensor ID for a Security Event ⌈

Type:	draft
Description:	The Security Extract shall support the definition of a security sensor ID for a Security Event.
Rationale:	It shall be possible to associate a security event with the numerical identifier of a security sensor.
Use Case:	Identify the source of a Security Event
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00009] Support optional Context Data for Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the definition of optional context data specific for a Security Event.
Rationale:	It shall be possible to configure that a given Security Event is reported with additional context data.
Use Case:	Report a Security Event with additional context data
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00002] Filter Chains for Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the definition of filter chains for Security Events.
Rationale:	It shall be possible to chain filters for Security Events such that a multi-stage filtering composed of several algorithms can be implemented.
Use Case:	Filter Security Events
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00003] Limitation Filtering for Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the definition of limitation filters for Security Events.
Rationale:	It shall be possible to limit further processing of Security Events in order to prevent exceeding capabilities of subsequent processing stages.
Use Case:	Limit Processing Load caused by Security Events
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00012] Pre-Qualification Provision for Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the definition whether pre-qualification is provided for a specific Security Event or not.
Rationale:	Alternatively to qualification by filtering, a (smart) sensor shall be able to report pre-qualified Security Events that shall directly be processed as qualified Security Events by the IdsM.
Use Case:	Report Pre-Qualified Security Events
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00004] Association of Security Event with an ECU/Machine ⌈

Type:	draft
Description:	The Security Extract shall support the definition of a relation between Security Events and the ECU on which they are detected and reported.
Rationale:	It shall be possible to configure that a given Security Event is reported by a given ECU
Use Case:	Report a Security Event on a given ECU
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00008] Association of Security Event with a Platform Module ⌈

Type:	draft
Description:	The Security Extract shall support the definition of a relation between Security Events and a platform module that is the subject of the security issue. A platform module is a basic software module (for Classic Platform) or a functional cluster (for Adaptive Platform)
Rationale:	It shall be possible to configure that a given Security Event is reported for a given platform module.
Use Case:	Report a Security Event for a given platform module
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00005] Association of Security Event with a Communication Bus ⌈

Type:	draft
Description:	The Security Extract shall support the definition of a relation between Security Events and a communication bus if the Security Event is used to report issues with regard to the related communication bus.
Rationale:	It shall be possible to configure that a given Security Event is reported for a given communication bus.
Use Case:	Report a Security Event for a given communication bus
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00021] Association of Security Event with an Application ⌈

Type:	draft
Description:	The Security Extract shall support the definition of a relation between Security Events and applications (Software Components for Classic Platform or Adaptive Applications) that are subject of the security issue.
Rationale:	It shall be possible to configure that a given Security Event is reported by a given application.
Use Case:	Report a Security Event for a given application
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00006] Support the Persistent Storage of Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the configuration of persistency for given Security Events.
Rationale:	It shall be possible to configure that a given set of Security Events is stored persistently on the ECU where it has been detected.
Use Case:	Store a Security Event on the ECU where it has been detected
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00007] Definition of Default Reporting Modes for Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the configuration of default reporting modes with different levels of details for the Security Events.
Use Case:	Report Security Events with different levels of details
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00018] Support definition of Severity Levels at Mapping of Security Events ⌈

Type:	draft
Description:	The Security Extract shall support the definition of severity levels individually for Security Events when they are mapped to an ECU or a machine.
Rationale:	It shall be possible to configure the severity levels for Security Events depending on their mapping to IdsM instances.
Use Case:	Report a Security Event with additional severity level information
Dependencies:	–
Supporting Material:	

⌋()

2.2 Requirements related to IdsM instances

[RS_SECXT_00013] Optional Configuration of IdsM Instances ⌈

Type:	draft
Description:	The Security Extract shall support the optional definition and partial configuration of one or multiple IdsM instances independent of whether each respective IdsM instance will run on Adaptive or on Classic Platform.
Rationale:	The Security Extract shall contribute partially to the configuration of IdsM instances in addition to Security Events
Use Case:	Optionally define and partially configure IdsM instances
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00014] Optional Configuration of Timestamp Provisioning ⌈

Type:	draft
Description:	The Security Extract shall support the configuration whether an IdsM instance provides timestamp information for reported Security Events and, if it does, whether this timestamp information is in AUTOSAR standardized format or not.
Rationale:	It shall be configurable whether an IdsM instance adds timestamp information to its reported Security Events or not.
Use Case:	Optionally report timestamp information for Security Events
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00015] Configuration of Timestamp Format ⌈

Type:	draft
Description:	The Security Extract shall support the configuration which format the IdsM uses when adding timestamp information to reported Security Events. The timestamp format can potentially be AUTOSAR standardized, standardized by other authorities, company-standardized or arbitrarily defined.
Rationale:	Different companies and projects are expected to use different timestamp formats for reported Security Events
Use Case:	Report timestamp information with configurable format
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00016] Optional Configuration of Authentication Provisioning for Security Event Messages ⌈

Type:	draft
Description:	For both the AUTOSAR Classic and Adaptive Platforms, the Security Extract shall support the optional configuration of requiring an IdsM instance to add authentication information (i.e. a signature) to all Security Event messages it sends onto a network.
Rationale:	The Security Extract shall support the IdsM instance configuration in terms of network configuration.
Use Case:	Optionally define and partially configure an IdsM instance on Adaptive Platform
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00017] Association of Network Configuration to an IdsM Instance ⌈

Type:	draft
Description:	For both the AUTOSAR Classic and Adaptive Platforms, the Security Extract Template shall describe how the association of an IdsM instance with its network configuration is to be defined.
Rationale:	The Security Extract shall support the IdsM instance configuration in terms of network configuration.
Use Case:	Optionally define and partially configure an IdsM instance
Dependencies:	–
Supporting Material:	

⌋()

2.3 Requirements related to AUTOSAR Methodology

[RS_SECXT_00019] Support definition of IDS scope and system boundaries ⌈

Type:	draft
Description:	The Security Extract shall support the definition of the scope (i.e. the system boundaries) of an IDS under design and implementation.
Rationale:	An IDS design typically involves a subset of all ECUs inside a vehicle. Each ECU of this subset shall be able to report individually defined and/or adapted security events. Therefore, for development of an IDS, the Security Extract needs to be able to define all system parts belonging to an IDS and the specific system-level capabilities of these IDS system parts.
Use Case:	System-level description of an IDS
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00020] Support partial and complete exchange of Security Extract definitions ⌈

Type:	draft
Description:	The Security Extract shall support partial as well as complete exchange of its definitions between development partners.
Rationale:	To enable distributed development of an IDS, multiple development partners contribute to a Security Extract file describing the whole IDS design. These contributors need to be able to specify their part of the Security Extract as independently of the others as the IDS design allows.
Use Case:	Distributed development of an IDS
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00010] Derivation of related ECU-C parameters ⌈

Type:	draft
Description:	The Security Extract shall support the derivation of ECU-C parameters related to Security Events for the IdsM module.
Rationale:	The Security Extract, being on system (M2) level, has to provide the required information to derive the configuration parameters (M1 level) related to Security Events for the IdsM module of an ECU. Regarding the AUTOSAR Methodology, it is therefore similarly used as the Diagnostic Extract or the ECU Extract.

▽

△

Use Case:	Derive ECU-C configuration parameters for IdsM
Dependencies:	–
Supporting Material:	

⌋()

[RS_SECXT_00011] Specification of AUTOSAR Standardized Security Events ⌈

Type:	draft
Description:	The Security Extract shall support specification of AUTOSAR standardized Security Events.
Rationale:	Together with the introduction of the Intrusion Detection System Manager, AUTOSAR will also provide standardized Security Events for existing BSW modules (Classic Platform) or Functional Clusters (Adaptive Platform). These standardized Security Events shall be specified using the Security Extract Template to enable automatic processing for document generation (single source principle).
Use Case:	Specify AUTOSAR standardized Security Events
Dependencies:	–
Supporting Material:	

⌋()

A History of Constraints and Specification Items

A.1 Constraint History of this Document according to AUTOSAR R20-11

A.1.1 Added Traceables in R20-11

Number	Heading
[RS_SECXT_00001]	Security Event
[RS_SECXT_00002]	Security Event Filtering
[RS_SECXT_00003]	Association of Security Event with an Ecu
[RS_SECXT_00004]	Association of Security Event with a communication bus
[RS_SECXT_00005]	Support the persistent storage of security events
[RS_SECXT_00006]	Support different reporting modes for security events
[RS_SECXT_00007]	Association of Security Event with a basic software module

Table A.1: Added Traceables in R20-11

A.1.2 Changed Traceables in R20-11

none

A.1.3 Deleted Traceables in R20-11

none