1 Purpose

This document describes the restrictions of MICROSAR OS SafeContext compared with the AUTOSAR specification and the Vector OS feature set.

2 Application area

All projects with operating system MICROSAR OS SC3 or MICROSAR OS SafeContext. Normally these projects are safety relevant ECUs (ISO 26262).

3 Target

Due to safety aspects, not all requirements of the AUTOSAR specification are implemented. This document describes the restrictions.

4 Supported Use Cases

Only applications based on OS scalability class SC3 or SC4 will be supported.

5 Features not supported

Class	Description

OS service API	`TerminateApplication`
	`CheckISRMemoryAccess`
	`CheckTaskMemoryAccess`
	`GetAlarmBase`
	`StartScheduleTableSynchron`
	`SyncScheduleTable`
	`SetScheduleTableAsync`

Internal Resources	Internal Resources are not supported.
Killing	“Killing” of Tasks or Applications is not supported. The only allowed protection reaction in the `ProtectionHook` is `PRO_SHUTDOWN`. Other reactions will be interpreted as `PRO_SHUTDOWN`. A missing TerminateTask error always causes shutdown.
OS Hooks	`ISRHook` `PreAlarmHook`

OS Application specific Hooks	`StartupHook<`*`Applicationname`*`>`
	`ErrorHook<`*`Applicationname`*`>`
	`ShutdownHook<`*`Applicationname`*`>`

Class	Description
Address Parameter Check	In case API functions with out-parameters (parameter passed by reference, e.g. GetEvent, GetAlarm, …) are called with illegal address-parameter, they do not return with the error code E_OS_ILLEGAL_ADDRESS as required by the AUTOSAR specification. Instead the out-parameter is written with the access rights of the caller, which may lead to a memory protection violation in case the given pointer is invalid.
Stack optimization	Stack sharing is not supported. Single stack model is not supported.
Internal trace	The “Internal Trace” feature is not supported.
COM	OSEK COM inter task communication with messages is not supported.
ORTI	`ORTIVersion = 2.0` is not supported.
Error Hook	`ErrorInfoLevel = Modulenames` is not supported.

Table 5-1 Not supported Features

6 Features with restricted usage

Class	Description
Interrupt resources	Resources are only available at task level, not in interrupt service routines.
OS Hooks	The following hook functions are limited: `PreTaskHook` is available for debugging only and must not be used in final code. `PostTaskHook` is available for debugging only and must not be used in final code.
Address Parameter Check	In case API functions with out-parameters (parameter passed by reference, e.g. GetEvent, GetAlarm, …) are called with illegal address-parameter, they do not return with the error code E_OS_ILLEGAL_ADDRESS as required by the AUTOSAR specification. Instead the out-parameter is written with the access rights of the caller, which may lead to a memory protection violation in case the given pointer is invalid.

Configuration Aspects	The following hooks must be always enabled:
	`StartupHook`
	`ErrorHook`
	`ShutdownHook`
	`ProtectionHook`

	For `SCALABILITYCLASS` only the settings SC3 or SC4 are supported. Memory protection must be active always.
	`STACKMONITORING` must be enabled.
	`OSInternalChecks` must be configured to Additional.

Table 6-1 Supported Features with restricted usage