

Limitations of MICROSAR RTE for Partition Termination

Version 1.0.0

2017-08-15

Application Note AN-ISC-8-1211

Author	Jonas Wolf
Restrictions	Customer Confidential – Vector decides
Abstract	This application note describes the scenarios it is considered possible to terminate an OS application, in which the MICROSAR RTE is used, using the MICROSAR OS.

Table of Contents

1	Overview	2
2	Limitations of MICROSAR RTE	2
3	Additional Resources	3
4	Contacts	3

1 Overview

Terminating and restarting of partitions (i.e. OS applications) is an AUTOSAR feature supported by Vector's Operating System (OS). Vector's MICROSAR Runtime Environment (RTE), however, does not implement termination or restart of partitions.

2 Limitations of MICROSAR RTE

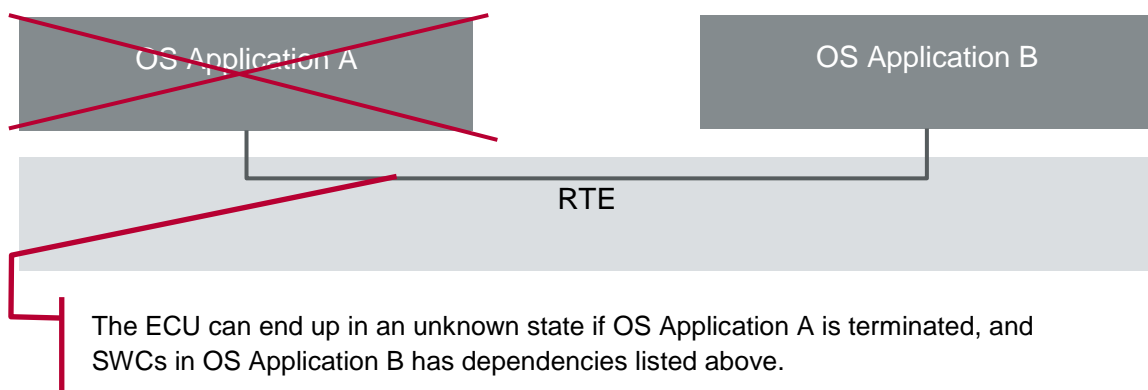
Terminating or restarting OS applications is problematic, for example when the following dependencies between different OS applications exist:

- > Trusted function calls,
- > Client/server communication,
- > Queued sender/receiver communication,
- > Mode management,
- > Dependencies on states on application level

These kinds of dependencies rely on either OS objects, like events, or RTE states, e.g. queue state. If one OS application is restarted, the other OS application(s) may have an inconsistent view on these objects or states. There may be also dependencies on the application level that are not obvious to identify, e.g. due to functional dependencies.

For implementing termination or restarting of OS applications it must be considered that termination or restart may happen exactly at a point in time when one of the activities above is being executed, e.g. during a client/server call.

The restarted OS applications need to establish their initialization state again. This requires initializing all variables, e.g. states and inter-runnable variables to their initial values. Due to a different system state in other partitions, this will most likely break functionality if no measures on the application level are taken.



The MICROSAR RTE currently does not implement functionality for terminating or restarting of OS applications. However, using the MICROSAR OS to terminate an OS application, in which the RTE is used, is considered possible only under the following conditions:

- > The OS application is only terminated and not restarted. Restarting the OS application requires a restart of the complete ECU.
- > The OS application, that is terminated, only has unqueued sender/receiver communication to other OS applications.
- > The OS application that is terminated, does not access other OS objects, like events, from other OS applications.

Please note that the OS unlocks any locked spin-locks, if an OS application is terminated. This may leave the protected data in an inconsistent state.

3 Additional Resources

VECTOR TECHNICAL REFERENCES

Technical Reference RTE

Technical Reference OS

4 Contacts

For a full list with all Vector locations and addresses worldwide, please visit <http://vector.com/contact/>.