ETAS

RTA FSQP 3.2.0

Release Notes

Copyright

Document RTA FSQP V3.2.0 R01 EN – 03.2019

Contents

1 Introduction

1.1 Definitions and Abbreviations

ASIL
: Automotive Safety Integrity Level

FSQP
: Functional Safety Qualification Package

OS
: Operating System; in particular, the AUTOSAR operating system.

RTE
: Run-Time Environment

TCL
: Tool Confidence Level

TD
: Tool Error Detection Level

TI
: Tool Impact Level

1.2 Package Overview

The RTA FSQP contains a number of documents to support the user in developing a safety case for their project. The different documents and their use cases are as follows:

Safety Manuals

The following three safety manuals are included in the RTA FSQP

- RTA-BSW Safety Manual
- RTA-RTE Safety Manual
- RTA-OS Safety Manual

These manuals contain guidelines and instructions on using the products in an ASIL environment. This consists of two main parts:

1. Assumptions on environment that need to be satisfied

   I.e. RAM has ECC…

2. Assumptions on Use that need to be performed by the user

   I.e. Callouts for X need writing

These assumptions needs validating in the context of the users development environment to form a coherent safety case.

RTA-BSW Safety Case

The RTA-BSW Safety Case consists of two parts

1. Evidence of the ASIL-D compliant process that the BSW modules were developed to. This includes an index of documents such as:
   - Work Instructions
   - Training Guides
   - Templates
   - Checklists
   - …
2. Evidence for <u>each</u> module that the process was followed in the form of an index of output artefacts such as:
   - Requirement Documents
   - Design Documents
   - Test Specifications
   - Tracing Reports
   - …

These evidences can form part of the user's safety case if required. For example referencing a modules evidences to reduce the requirement to produce software designs.

Tool Certificates

A copy of the current valid TuV Certificates for RTA-RTE & RTA-OS are provided. These certificates state that these tools are fit for purpose to develop safety related software According to IEC61508 and ISO26262.

The current validity of these documents, ensured by yearly Factory Surveillance Audits by TuV, may be checked by suppling the certificate number into the following website:

https://www.tuev-sued.de/product-testing/certificates

These may be used as-is, or can be used to argue applicability for other IEC61508-based standards such as ISO25119.

Tool Pre-Classification Reports

The FSQP includes a set of tool Pre-Classification reports. The user must verify that their environment matches that described in the Pre-Classification report before being used as a Classification report. The Pre-Classification reports cover the following points:

- Overview of the assumed development process in which the tools will be used
- An enumeration of assumed use-cases
    - The possible error cases and measures to mitigate these error cases for each of these use-cases
    - An assignment of a Tool Classification Level for each use-case based on a set of obligations being fulfilled.
- An overall Tool Classification Level based on the all the above use-cases

If the development process and scenarios are verified as being the same as the users environment, and the obligations are fulfilled, then these reports may be used as actual classification reports. If there are any deviations in development process then modifications should be made in accordance to ISO26262 before using these as Classification reports.

Safety Audit Reports

To ensure that the work products above meet the requirements of ISO26262 an independent audit of the work products is conducted. This audit is based around spot-checks and ensures, amongst other things that:

- Safety Manuals are fit for purpose
- Safety Case process described is ASIL-D compliant
- Safety Case Work Products comply to the process described
- Tool Pre-Classification reports look fit for purpose

2 Change History

2.1 Version 3.1.0

Version 3.1.0 of the RTA FSQP is intended for use with v3.1.0.0 of RTA-BSW. The changes based on the previous RTA FSQP is as follows.

Updated

This FSQP contains new versions of the following documents:

- RTA-BSW Safety Manual
- RTA-BSW Safety Case

Added

The following new documents were added:

- Tool Pre-Classification Reports
- TuV Certificate (Z10 13 08 34489 004) for RTA-OS and RTA-RTE
- RTA-RTE V6.6.0 Safety Manual
- RTA-OS v5.6 Safety Manual

In Progress

As the safety audit is still in progress the following documents will be provided in a future hotfix:

- Safety Audit Report

2.2 Version 3.2.0

Version 3.2.0 of the RTA FSQP is intended for use with v3.2.0 of RTA-BSW. The changes based on the previous RTA FSQP is as follows.

Updated

This FSQP contains new versions of the following documents:

- RTA-BSW Safety Manual
- RTA-BSW Safety Case

Added

The following new documents were added:

- RTA-RTE V6.7.1 Safety Manual
- RTA-BSW 3.1 Functional Safety Audit Report

3 Contacting ETAS

Support

The RTA hotline is available to all RTA users with a valid support contract:

Email (preferred)	rta.hotline.uk@etas.com
Phone (0900-1730 GMT/BST):	+44 (0)1904 562624

Please provide support with the following information:

- Your support contract number
- The name and version of the ETAS tools you are using
- Your relevant AUTOSAR XML configuration files
- Reproduction steps that result in the issue is applicable

General Enquiries - ETAS HQ

ETAS GmbH		
Borsigstraße 24	Phone:	+49 711 3423-0
70469 Stuttgart	Fax:	+49 711 3423-2106
Germany	WWW:	www.etas.com

General Enquiries - ETAS Subsidiaries

For details of your local sales office as well as your local technical support team and product hotlines, take a look at the ETAS website:

ETAS subsidiaries	WWW:	www.etas.com/en/contact.php
ETAS technical support	WWW:	www.etas.com/en/hotlines.php