Product Description

QKit IBM ENG

Version:	0.4
ID	722-Product-QKitIBMENG
Date:	15.07.2021
Status:	In Progress / Presented / **Reviewed** / Final
Author:	Dr. Oscar Slotosch
File:	E:\svn\ISO26262_TQ\trunk\PresentationBlocks\IBM\Product.docx
Size:	14 Pages

History:

Version	Date	Status	Autor	Change
0.1	2021-04-25	In Progress	Slotosch	Document created
0.2	2021-04-27	In Progress	Slotosch	First complete version, ready for review
0.3	2021-04-28	Reviewed	Slotosch	Added internal review feedback
0.4	2021-04-29	Reviewed	Slotosch	Added IBM feedback
1.0		Final	Slotosch	Finalized document

Contents

1 Scope of this Document

This document describes the Validas Qualification Kit for the IBM Engineering solution. The QKit is named "QKit IBM ENG" and allows to use the IBM Engineering solution with the required confidence within safety-related development projects compliant with relevant safety standards like [ISO 26262:2018], DO-178C with DO-330, [IEC 61508] and others.

This document is structured as follows:

- Section 2 describes the background and product positioning
- Section 3 shows the safety roadmap, i.e. the steps you have to perform to use the tool with the required confidence in safety projects.
- Section 0 describes how the QKit is applied to qualify the IBM Engineering solution
- Section 5 lists the contents of the QKit, i.e. the contained services and the contained artifacts to perform the qualification
- Section 0 provides further information about the QKit.

More details about the certified Validas Qualification Methodology can be found in [QMeth].

2 Background and Product Positioning

Tool Qualification Kits contribute to the safety and standard compliance of tools. Tools are used to develop safe systems and safe software.

Figure 1 shows an overview of the system safety and the required aspects of it.
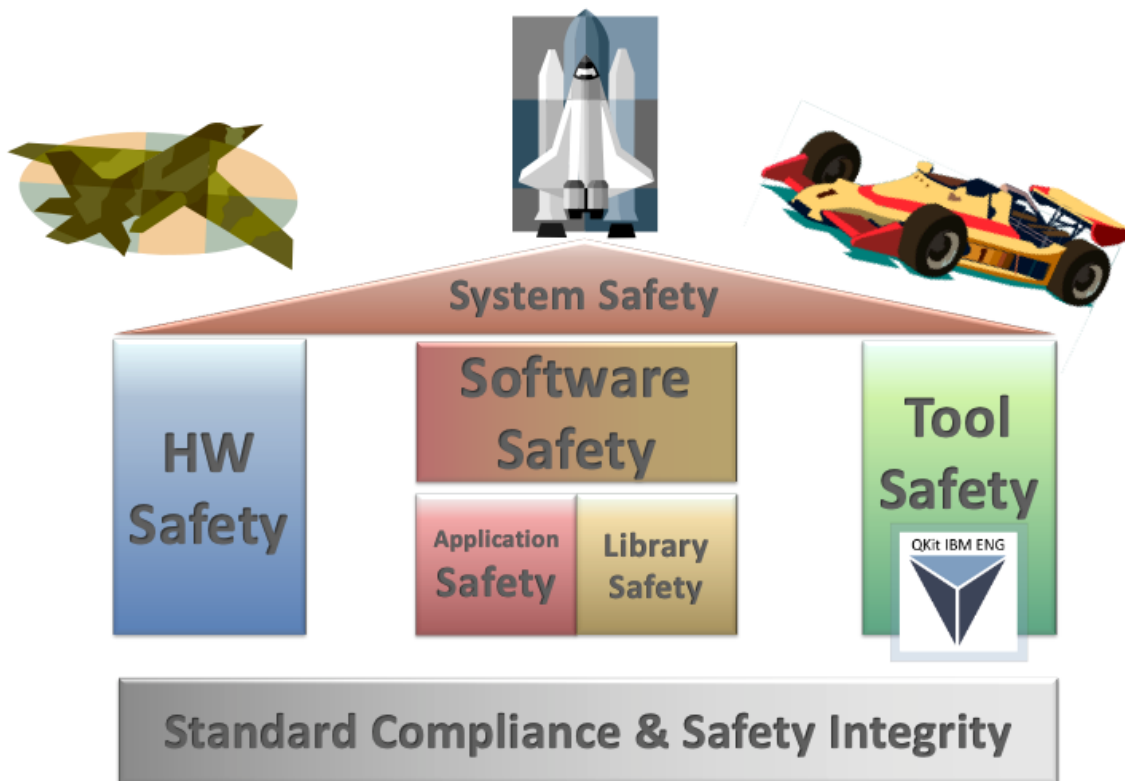

Figure 1: Safety Overview

3 Safety Roadmap for IBM Engineering solution

The safety standards like [ISO 26262:2018], [IEC 61508], and [DO330] require to define, follow and document a standard compliant process when developing a safe system. The definition of the process is contained in the **safety plan**, which is a process description that has to meet the safety requirements for the corresponding safety integrity level (SIL or ASIL). The documentation that the defined process was followed during product development is called **safety case**.

Since tools are used to develop the system, the selection, classification and optional qualification of the tools are part of safety planning and have to be performed before the tools are used to develop the safe product.

The development of the safe product has to use the tools safely. This is achieved by following a "**Tool Safety Manual (TSM)**", which is created during the classification and qualification of the tools and which guides the tool user to use the tool safety with the required confidence.

Tool classification and qualification has to be part of safety planning. This means that tool qualification of the IBM Engineering solution has to be done very early in the process, especially *before* building the product.
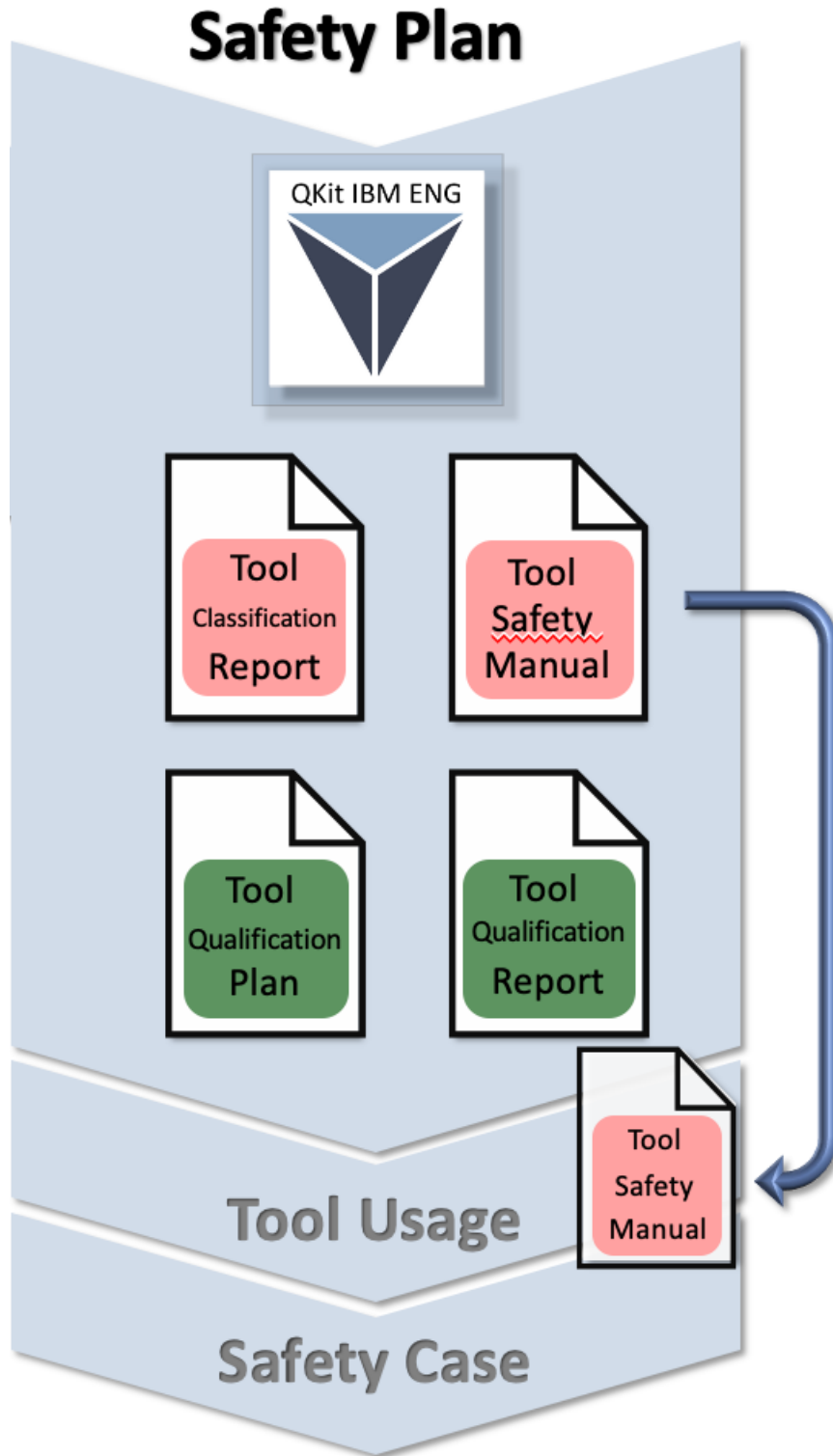
Figure 2: Safety Roadmap Phases

Figure 2 shows an overview about the safety planning process.

The QKit IBM ENG from Validas supports customers within this process by performing validation tests of the QKit IBM ENG tool site in the environment of the tool user and by providing the required documents, including the tool safety manual (TSM) that describes how to use IBM ENG tools safely. The TSM is generated from the QKit, based on the use cases and required tool features from the tool user.

The QKit IBM ENG is a growing qualification kit. This means it currently does not cover all tools & features of the IBM Engineering solution, but only parts of it. To ensure that the parts which are covered by the qualification kit suffice for the customer/tool user the use cases that the customer has need to be specified. In case the customer uses more IBM Engineering features within his use cases the QKit needs to be extended ("tailoring"). This step is done from Validas before delivering the QKit to the customer. Prerequisite for the tailoring is a **Use Case Definition Workshop** that the customer has to buy from Validas before the QKit can be delivered.

So in total the **roadmap** for building a safe product using the IBM Engineering tools is as follows:

0. Decide to **use** IBM Engineering solution
1. Decide to use IBM Engineering solution as **part of the safety process**. In case any of the IBM Engineering solution is mentioned within the product safety plan, e.g. "Safety requirements are managed using DOORS Next", the tools contribute to the safety plan and safety case of the product and require to be classified and qualified for safety.
2. **Contact Validas AG** for QKit IBM ENG by sending an email to qkitsupport@validas.de
3. **Safety Planning** with Validas and the QKit IBM ENG. The safety planning includes tool classification and qualification and consists of several substeps:
   a. **QKit IBM ENG product presentation** (cost free webex). Here Validas AG demonstrates the safety requirements, the used tool qualification method (Validating QKit) as well as the tailoring process. Next steps are planned if desired.

b. **Customer Use Case Workshop** with Validas. Within this workshop (or some online-meetings), we will perform the following steps to see if the QKit IBM ENG covers the use cases of the customer:

  i. **Identify Use Cases:** Typically a use case is a set of tool functions that are used within a team or development phase, for example "System Requirement Management" is the use case and the used tool features could be "Create Requirement", "Link Requirements", "Filtering", "Dashboard" ,..

  ii. **Plan Qualification:** The qualification consists of the application of the QKit IBM ENG (see Section 0) and of the tailoring which might be necessary to cover the customer use cases. Hence there are the following two steps

   1. **Tailoring & Extension:** Within tailoring & extension the QKit IBM ENG is compared with the identified use cases. In case some features are missing or some safety guidelines are not acceptable from the tool user the QKit will be extended and tailored towards the need of the tool user

   2. **Application:** The application of the QKit is planned. This involves determination of the environment, parameters and access rights.

  iii. **Plan Tool Usage:** The tool usage has to follow the tool safety manual that will be generated from the tailored QKit IBM ENG. Based on the qualification plan we can predict the structure and contents of the expected tool safety manual with safety guidelines that will be the generated output of the tailored QKit. Those guidelines can be judged from the tool user and eventually require additional tailoring of the QKit.

c. **Order QKit IBM ENG:** Based on the proposed tailoring and additional required extensions Validas will create an offer for the tailored QKit IBM ENG. If the tailoring, support and the extensions cannot be done within the support efforts that are contained in the QKit (see Section 4), Validas AG will create an extended offer to adapt the QKit to the wishes of the customer. If desired Validas AG can also offer a "TÜV certificate" documenting the standard compliance.

d. **Receive (tailored) QKit IBM ENG:** some weeks after the order Validas will deliver the updated, tailored QKit.

e. **Apply QKit IBM ENG:** The application of the QKit will produce the required documents: Tool Classification Report, Tool Qualification Plan & Report and the Tool Safety Manual. The generated documents can be submitted to Validas for confirmation review. The tool qualification can be archived for documentation purpose.

4. **Safe Usage**: Once the safety planning including tool qualification is done, the product can be developed safely using the IBM engineering tool suite with the required confidence by following the generated tool safety manual from the application of the QKit. The safe tool usage has to adhere to the tool qualification safety manual. This needs to be documented somehow. Validas proposes to use an Excel sheet and to create a safety tool usage report (SUR).

5. **Safety Case**: The safety case is t e collection of all documents that witness that the product is safe, i.e. the usage of the IBM Engineering solution was compliant with the safety plan (tool safety manual).

4 Application of the Qualification Kit

The application is done within the customer environment. It is done using the Qualification Support Tool (QST), which is part of QKit IBM ENG. Input of the qualification is the IBM Engineering solution together with the current configuration parameters and the specification of the use cases. Also, the required safety guidelines have to be confirmed during qualification. Based on this output the QKit generates all safety documents and thus makes the tool ENG safely usable within safety relevant projects. Figure 3 shows this graphically.
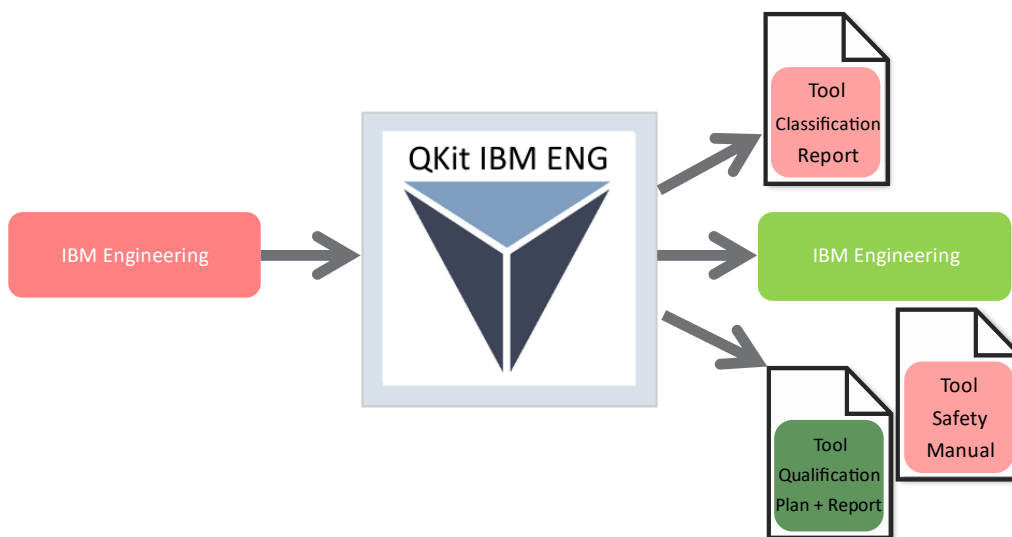

Figure 3: Application of QKit IBM ENG

The generated documents can be submitted to Validas for confirmation Review.

5 Application of the Qualification Kit

5.1 Contents & Release Plan of QKit IBM ENG

The QKit IBM ENG is a growing QKit, i.e. it does not cover all tools and features contained in the IBM Engineering solution right now, but it is constantly increasing based on customer needs. There are three degrees of coverage within the QKit

- Feature is not covered
- Feature is covered with a risk analysis and safety guidelines to use the feature safely by detecting it's potential errors.
- Feature is covered by validation test cases that can show that the potential errors

Figure 4 shows an overview of the DOORS Next features within the QKit in April 2021.

Beside the specifications, guidelines and test cases the QKit IBM ENG contains the followings things:

- User Manual & First Step Presentation
- Qualification Support Tool (Document Generator & Templates) for
    - Tool Classification Report (TCR)
    - Tool Qualification Plan (TQP)
    - Tool Qualification Report (TQR)
    - Tool Safety Manual (TSM)
- Test Automation Unit to run test cases in the user environment
- Test Cases for the "testable" features
- Compliance Report(s) for the following standards
    - ISO 26262
    - IEC 61508
    - DO-330
- Verification & Validation Report to show the compliance
- Release Notes of QKit IBM ENG (including QKit Issues)
- 10 days of Validas Qualification/Extension Support
- The Pre-Qualified & certified version of the QKit IBM ENG also contains
    - Reviewed, ready to use documents (TCR, TQP, TQR, TSM)
    - TÜV certificate

The roadmap for the growing QKit depends on the number of customer tailoring and extending it. As an outline we have the following milestones defined:

- 2020/12: "CupCake+": First benchmark (demo) from IBM running test cases and handling global configurations (streams)
- 2021/06: "Mitigatable Complete Version": covers main features and tools (mostly with mitigations) and some pilot users

- 2021/12: "Partially testable Version": A version that contains some significant amount of test cases that reduce the number of necessary safety guidelines

- 2022/06: "More testable Version": A version that contains even more test cases for the IBM Engineering solution and features.

6   Contact & Further Information

The following further information is available:

6.1   Product Overview

An   overview   about   the   product   is   available   on   the   internet   at
http://www.validas.de/en/products/#elm

6.2   Contact

For further information, concrete offers, etc. feel free to contact Validas using mailto:
qkitsupport@validas.de

6.3   Podcast

Validas AG produces a podcast about tool & library qualification. It is available in most podcast
stores like iTunes, Spottify, ..

See also in http://www.validas.de/en/podcast/

In season 2 the episode 7 Oscar Slotosch explains the QKit IBM ENG.

7 References

[DO330] RTCA. DO-330: Software Tool Qualification Considerations 1st Edition 2011-12-13.

[EN50128]: BS EN 50128:2011, Railway applications — Communication, signaling and processing systems — Software for railway control and protection systems, BSI Standards Publication

[[IEC 61508]] International Electrotechnical Commission, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, Edition 2.0, Apr 2010.

[ISO 26262:2018] International Organization for Standardization. ISO 26262 Road Vehicles – Functional safety–, 2nd Edition, 2018

[QMeth] Validas Tool Qualification Methodology, Version 2.3, April 2021