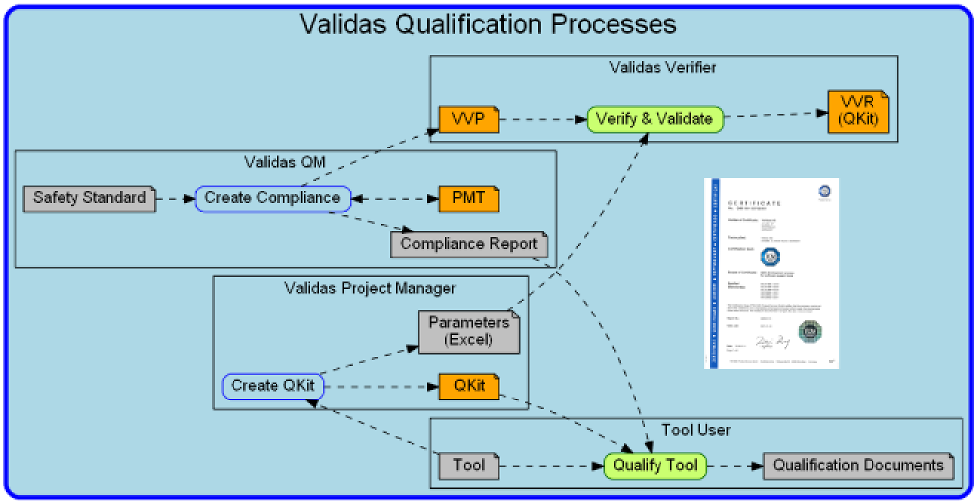
Overview: Safety Case for Cxx Standard Library Parts (<Customer>)



Version:	1.1
ID:	XXX-SCO-Cxx Standard Library Parts (<Customer>)
Date:	2020-11-11
Status:	Generic / Adapted / Reviewed / **Final**
Author:	Dr. Oscar Slotosch
File:	C:\Users\oscar\Desktop\SafetyCaseGeneric.docx
Size:	14 Pages

History:

Version	Date	Status	Autor	Change
0.1	2020/04/25	Generic	Oscar Slotosch	Template created
0.2	2020/04/25	Generic	Slotosch	Structure Created
0.3	2020/04/25	Generic	Slotosch	Content added
0.4	2020/04/26	Reviewed	Nasuh Isiktas	Reviewed Generic Proposal
0.5	2020/04/26	Generic	Oscar Slotosch	Added Review Feedback: typos, references and clarifications
0.8	2020/04/26	Adapted	Oscar Slotosch	Adapted to Validas AG
0.9	2020/04/26	Reviewed	Nasuh Isiktas	Reviewed Adaptation
1.0	2020/04/26	Final	Oscar Slotosch	Finalized
1.1	2020/11/11	Final	Oscar Slotosch	Anonymized from Customer

Contents

List of Figures

1 Scope of this Document

This document describes gives an overview about the safety case for ‘Cxx Standard Library Parts (<Customer>)’. It sketches the safety plan and the safety case. The safety plan is generated from the PMT model using the PMT tool. The safety plan can be re-used in different projects since it is parameterized.
The safety case is mainly generated from the TCA-SW tool, which contains a model of the software requirements, architecture and design, units, risks, mitigations as well as the test cases and parameters for calibration and configuration. The verification and validation is created using the V&V tool, which required the parameters from the created TCA-SW-Model in order to verify all elements (Requirements, Features, tests,..).

The safety case contains also the models (PMT, TCA, VVT) that are the source of almost all documents in the safety case.

The document has the following main chapters (preceded by a glossary and finished by a reference section):

- Safety Architecture (Section 3): describing the overview of safety plan and safety case
- Safety Case (Section 4): Describing the project specific documents of the safety case.

The general processes are described in the Validas Qualification Methodology [QMeth].

2 Glossary

The following abbreviations are used in the document. More information on the concepts & processes can be found in [QMeth].

- AOC: Anomalous Operating Condition
- Artifact: Element exchanged between processes
- Calibration (of SW): Parameters that are selected after the software has been deployed
- Configuration (of SW): Parameters that are selected before/during build process of the software
- CR: Compliance Report[1]
- CT: Construction Task (during QKit creation)
- DIA: Development Interface Agreement
- KB: Known Bug
- Library: Pre-Existing Software
- LCR: Library Classification Report
- LQP: Library Qualification Plan
- LQR: Library Qualification Report
- LSM: Library Safety Manual
- LTG: Library Test Generator
- PCCP: (Development) Process Compliance Check Plan
- PCCR: (Development) Process Compliance Check Report
- Parameter: Selectable value (including its type)
- PMT: Process Modeling Tool
- Process Module: modular tasks in the process
- PR: Process Report
- PT: Preparation Task (before QKit creation)
- Role: see Stakeholder
- QKit: Qualification Kit: Collections of things that simplify qualification
- QP: Qualification Plan (general), can be LQP or TQP
- QR: Qualification Report (general), can be LQR or TQR
- QST: Qualification Support Tool: Automatizes Qualification Process
- SEOOC: Safety Element Out Of Context according to [ISO26262]
- SM: Safety Manual (general), can be LSM or TSM
- Stakeholder: abstract person taking over responsibilities in the process
- SWC: Software Component, e.g. a library[2]
- TAU: Test Automation Unit
- TCA: Tool Chain Analyzer: automatizes qualification tests (in QKit or elsewhere)
- TD: Tool Detection (part of TCL computation according to [ISO26262])

[1] Do not confuse with Classification Reports LCR and TCR.

[2] Note that a library (set of functions) can be qualified as unchanged software component (if unchanged) or as modified/changed SEOOC according to ISO 26262.

- TCL: Tool Confidence Level (according to [ISO26262])
- TCR: Tool Classification Report
- TI: Tool Impact (part of TCL computation according to [ISO26262])
- Tool: Software not being part of the product
- TP: Test Plan
- TQL: Tool Qualification Level (according to [DO330])
- TQP: Tool Qualification Plan
- TQR: Tool Qualification Report
- TR: Test Report
- TSM: Tool Safety Manual
- V&V: Verification and Validation
- Validation: Checks if the right product is build, i.e. qualification can be performed clear, easy and safe way (”customer satisfaction”)
- Verification: Checks if the product is built correctly, i.e. all requirements from the standards are satisfied (“standard compliance”)
- Verification Module: special form of Process module used to verify an artifact in the process
- VVP: Verification and Validation Plan
- VVR: Verification and Validation Report
- VVT: Verification and Validation Tool
- VT: Verification task (after QKit creation)

3 Safety Architecture

This section describes the structure of the safety case. It consists of a safety plan describing the process and a safety case describing the successful execution of the process to show the safety of Cxx Standard Library Parts (<Customer>).

The safety plan (left side of Figure 1) is derived using the Validas compliance method from the process model using the process modeling tool, see [QMeth]. It consists of

- DIA: Development interface agreement (DID_DIA),
- Process Report (DID_PR) with the description of the process,
- Compliance Report (DID_CR) with the compliance argumentation for all requirements and the corresponding criteria to verify and validate them
- Compliance overview table (DID_CR_TAB) with the compliance elements of DID_CR
- Documentation Management Plan (DID_DOCPLAN) describing the documents of the safety plan and case with the responsible persons
- Documentation Management Table: Table to manage the creation, review and finalization of the documents within the project.
- Verification and Validation Scheme: The VVT-model from which the V&V Plan (and the V&V Report) is generated within the project. This is done by "instantiating" the scheme using the process parameters that are exported from the modeling tool (Tool Chain Analyzer of the software – TCA-SW)

All documents of the safety plan are generated from the safety expert using the Process Modeling Tool (PMT).

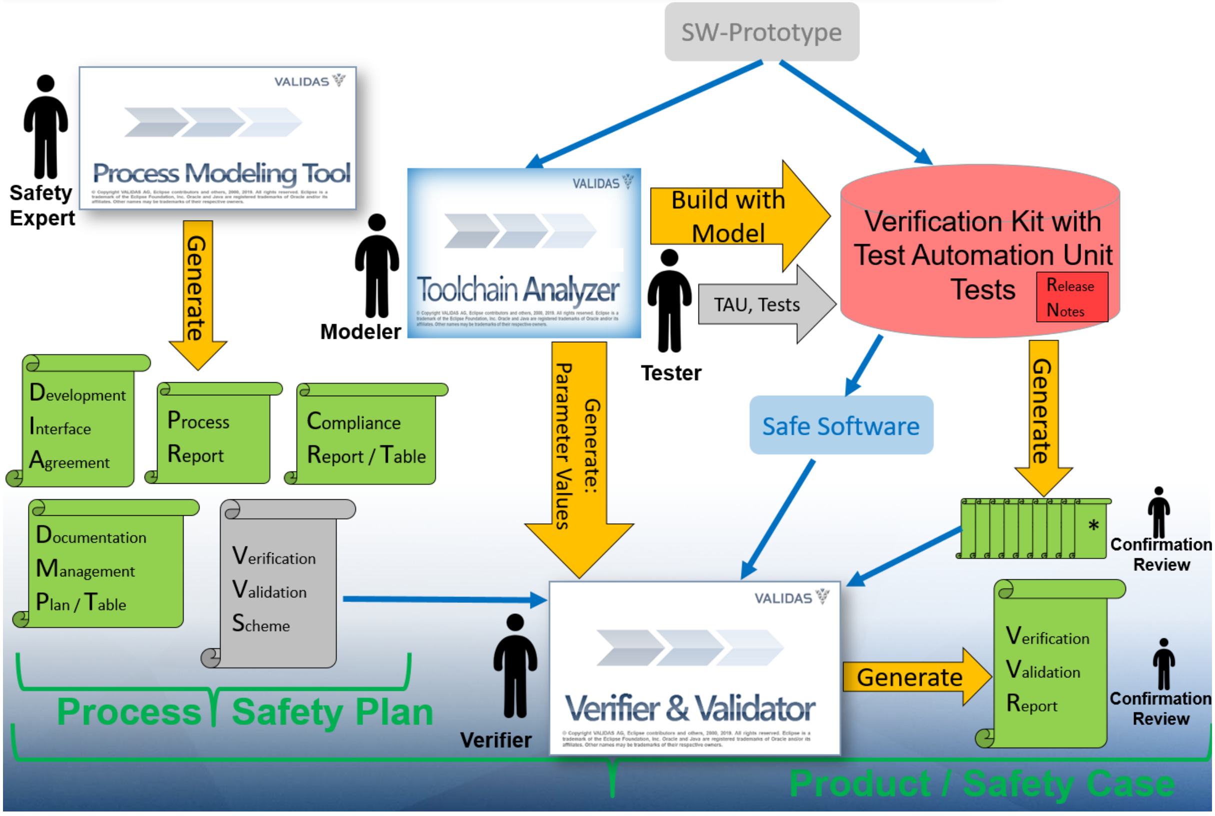


Figure 1: Structure of Safety Case

The safety case extends the safety plan by many documents (see Section 4). It is created by building a TCA model for the software (prototype) and going through all required software engineering phases (requirement to tests), including the required safety analyses, see Section 4 for the resulting documents and the developer guide (DID_DG) for more details.

The TCA model contains also test specification (test strategies). The TCA model, the implemented tests and a Test Automation Unit / TAU (from the tester) are integrated into a Verification Kit that can be used to verify the software on the target as required from the standards and that generates many project specific documents, see Section 4. The verification kit contains also release notes that specify eventual restrictions to be considered when verifying or using the software such that it can be used safely.

The Verification and Validation is done using the V&V Tool by combining the VVS with the parameter values exported from the TCA, since some checks have to be repeated for each value of the parameter (e.g. for every requirements or for every test).

The confirmation reviews do not replace the assessment of the safety case, but check the document generators, since they are currently TCL1.

4 Safety Case

The documents of the safety cases are structured in Figure 2 according to the development process and how they are used (user & developer guide: DID_QKIT_UG / DID_QKIT_DG as well as the TCA model DID_TCA_MDL) and generated. It is structured according to the software development process (V-model of [ISO26262] with product specific supporting processes). The process related documents of the safety case (safety plan) are described in the previous section 3.

The blue arrows denote the inputs to the verification kit that the verifier uses to verify the software on the hardware by using the hardware software interface (HSI) and the test automation unit TAU according to the user guide (DID_QKIT_UG) and executes the specified test cases in the TCA model. The TCA model also contains further information about the software (requirements,architecture,tests, tools) that the developer has modeled there according to the developer guide (DID_QKIT_DG).

The orange arrows denote document generation of the VKit. The document colours in Figure 2 indicate the requirements classes from the safety standards:

- Red: document is required for the software that is developed according to the safety standard
- Yellow: document is required for the used (unchanged & pre-existing) library software components
- Green: document is required to create the confidence into the used development and verification tools.

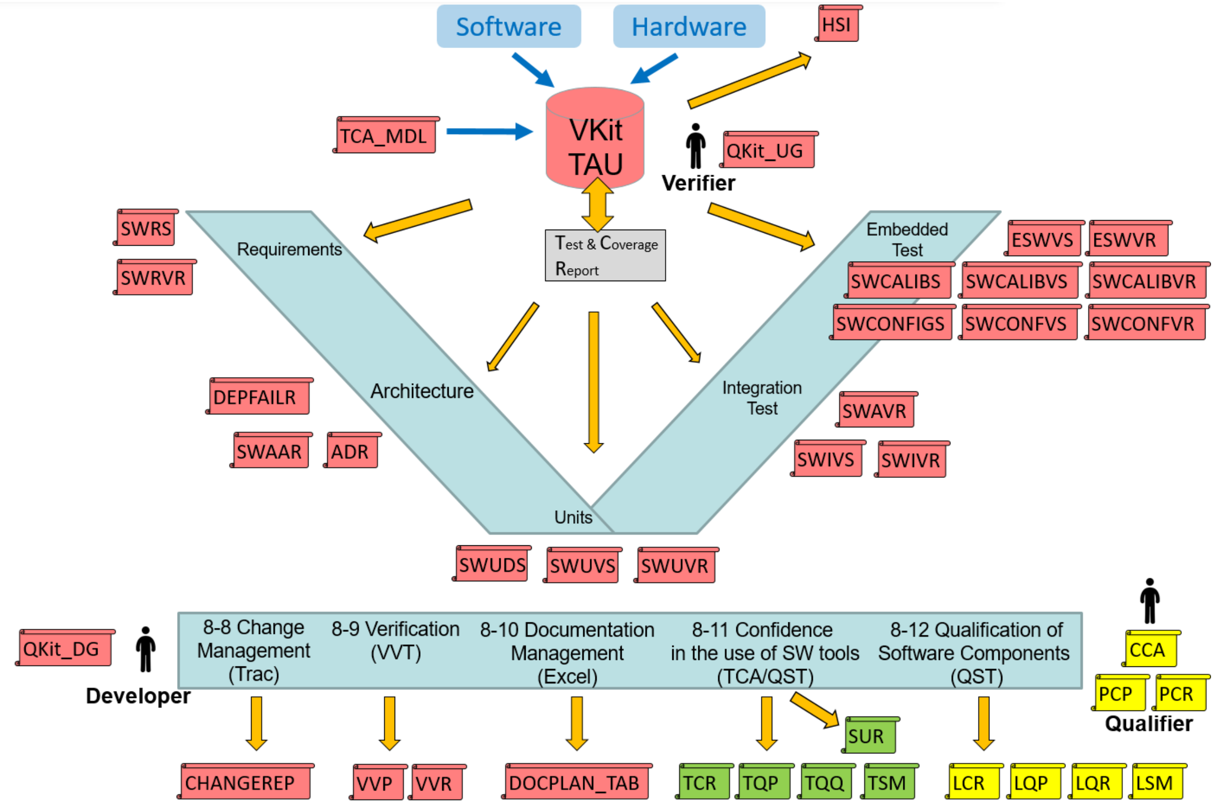


Figure 2: Documents in Safety Case

The grey artifacts that are generated from the TAU are no documents in the sense of the safety standard, but provide input to the generation of the other documents. They can be used to check the correctness of the generated documents

The documents in Figure 2 are structured according to their process (V-Model with supporting processes[3]). More information about them can be found in the documentation management plan (DID_DOCPLAN) and the Validas qualification methodology [QMeth]:

- Requirements documents: describe the functional requirements (Use Cases of the software) together with the safety requirements / risks (potential errors) that shall be avoided.
- Architecture documents: describe the component structure of the software together with data and control flow.
- Software Unit documents (specification / verification specification / verification report) describe the specification of the atomic components (Units), their test cases and their test results
- Integration test documents: describe the verification of the hierarchic components (review and tests with specification and result)
- Embedded test documents: contain the results of testing the complete software embedded on the target. Beside the requirements tests, this includes also the specification and tests of calibration and configuration parameters[4] (if applicable).
- Change report (DID_CHANGEREP): is generated from the used change management system (trac) by exporting all issues and tasks into a template (DID_CHANGEREP_MP).
- Verification and Validation documents: are created using the VVT tool after performing the V&V activities specified in the safety plan (see Section 3)[5].
- Documentation management table (DID_DOCPLAN_TAB): is created from PMT and manually updated to manage and document the status of the delivered documents.
- Tool confidence documents: are created from the TCA model (DID_TCA_MDL) or other qualification kits, e.g. for the compiler since the used tools are also modeled there (except the pre-qualified tools). This has to be done before verifying the software (part of safety planning) in order to follow the safety manual (DID_TSM). The tool qualification documents (DID_TQP and DID_TQR) are

[3] Note that the other supporting processes are omitted from this image, since they are related to the process and therefore handled in the safety plan in the previous section 0.

[4] Configuration parameters are changed before the software is build (e.g. #defines), while calibration parameters are changed in the build software (e.g. using a debugger / calibration tool).

[5] Note: V&V can be done in several phases based on the completion of the developed elements, however finalizing the V&V report is part of finalizing the safety case.

available in several instances for the qualified tools (compiler, test automation unit and TCA/QST). The safe tool usage report (SUR) documents that the tools have been used as classified and qualified.

- Component qualification documents: describe the qualification of the used pre-existing and unchanged software components. The library process compliance check report (DID_PCR) needs to be created manually from the corresponding library process compliance check plan (DID_PCP). The library code coverage analysis report (DID_CCA) is only required for ASIL D libraries and only if not 100% coverage is achieved during testing. If no libraries are used, these documents are not required and not generated.

Note that for simplicity and consistency the verification kit does not only generate the documents that depend on the test results (unit integration and embedded tests), but also the other documents (DID_HSI, requirements & architecture).

5 References

[CR] This compliance Report for ‘Cxx Standard Library Parts (<Customer>)’, generated by [PMT]

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

[DO178C] RTCA. DO-178C: Software Considerations in Airborne Systems and Equipment Certification, 2011-12-13.

[EN50657] BS EN 50657:2017, Railways Applications. Rolling stock applications. Software on Board Rolling Stock, BSI Standards Publication.

[FDA2002] General Principles of Software Validation; Final Guidance for Industry and FDA Staff, Jan 2002, from http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf

[FDA_OTS] Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices, Center for Devices and Radiological Health (CDRH), from http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm073779.pdf

[IEC61508]International Electrotechnical Commission, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, Edition 2.0, Apr 2010.

[IEC62304] International Electrotechnical Commission, IEC 62304, Medical device software –Software life cycle processes

[ISO26262] International Organization for Standardization, ISO 26262 Road Vehicles –Functional safety – 2nd Edition, 2018-12.

[PMT] Process Modeling Tool, available at http://www.validas.de/en/tools/ including a user manual contained in the documentation plugin of the tool

[PR] Process for Cxx Standard Library Parts (<Customer>), generated by PMT, DID_PMT, see <QKit>/Documentation/PR.pdf

[QMeth] Validas Qualification Method, White Paper, see <QKit>/Documentation/QualificationMethodology.pdf

[VVP] Verification and Validation Plan (Model) for Cxx Standard Library Parts (<Customer>), DID_VVS, generated by PMT

[VVR] Project specific Verification and Validation Report for Cxx Standard Library Parts (<Customer>), to be created by performing and

documenting [VVP], DID_VVR, contained in <QKit>/Documentation/VVR.pdf