S9.5 Part 5: Related Safety Cases

for the development of an STM ATB

Colophon	
Document ID	S9.5
Revision	539098
Author	A
Date:	2020/07/06 15:36

Authorization

Compiled by: AZB Signature/E-sign: 539098 ,STMA-79295	Date: 2020/07/06 15:51
Reviewed by: AGP Signature/E-sign: 539098 ,STMA-79276	Date: 2020/07/06 15:42
Approved by: AZB Signature/E-sign: 539098 ,STMA-79300	Date: 2020/07/06 15:58

Contents

1 Preface . . . 3
1.1 Introduction . . . 3
1.2 References . . . 3
2 Reference to Related Safety Cases . . . 3
2.1 TI RM48 MCU . . . 3
2.2 Xilinx Artix XC7A200T-1FBG484I . . . 4

1 Preface

1.1 Introduction

This part of the safety case refers to the related (i.e. underlying) safety cases.

1.2 References

Reference documents

All the documents references used in this document can be found in the document P6.1 Bibliography available in the Polarion folder Processes

Abbreviations, definitions and terminology

An overview of the abbreviations, definitions and terminology used in this document can be found in document P6.2 List of abbreviations, definitions and terms available in the Polarion folder Processes

Requirement identification

The STM ATB project makes use of an automated requirement management system. In this system each requirement has been identified as a work item. Each work item has been automatically assigned with a unique ID, with the format "STMA-<number>". As a result requirement ID's are not in logical order. An overview of all the used STMA-numbers is given in document P6.3 Requirement Overview available in the Polarion folder Processes

2 Reference to Related Safety Cases

2.1 TI RM48 MCU

The microcontroller selected as the functional processor, the Texas Instruments RM48x, is certified for SIL3 applications IEC 61508-1(ed.2), IEC 61508-2(ed.2).

Certificate No.	Reference
Z10 16 01 84071 009	SPNQ004B

In chapter 4.2 of the certification report the general conditions and restrictions for SIL3 are stated:

- The guidelines and requirements specified in the user documentation shall be followed. Especially the requirements of the system integration section of the Safety manual have to be regarded.
- The impact on the overall safety concept and the safety function has to be well understood and analysed if a safety mechanism described in the Safety Manual is not used.
- All safety mechanism implemented by the system integrator have to be developed and verified according to the targeted safety standard.
- All specific required characteristics and behaviour of the Safety MCU required by the final safety function have to

be developed and verified according to the targeted safety standards. This includes also timing aspects like reaction times, test intervals or test execution times.

- The system integrator has to make sure that the conditions and restrictions defined in the documentation of the Safety MCU are understood and followed."

To comply with the conditions and restrictions the guidelines and requirements from the following documents were followed:

Document	Reference
RM48L95216- and 32-Bit RISC Flash Microcontroller	SPNS177D
RM48x 16/32-Bit RISC Flash Microcontroller Technical Reference Manual	SPNU503C
Safety Manual for RM48x Hercules ARM-Based Safety Critical Microcontrollers User's Guide	SPNU577D
RM48x Microcontroller Silicon Revision D Silicon Errata	SPNZ223B

These requirements have been collected and listed in D5.1.5.1 SAP Board design items so that they can be traced to the design and implementation.
In D6.2.12 SDD Functional Processor Hardware Monitor can be found which test diagnostics have been selected and which custom test measurements have been implemented. The impact of the selected test diagnostics and custom test measurements can be found in D6.9.3 FMEDA Hercules and Companion Chip.

2.2 Xilinx Artix XC7A200T-1FBG484I

The Xilinx Artix XC7A200T-1FBG484I is qualified to meet applicable requirements with the IEC 61508 safety standard. The Vivado Design Suite is certified to support safe and secure FPGA designs according to IEC 61508010 and ISO 26262:2011.

A Device Reliability Report [UG116] is available.

Xilinx Vivado tooling certificate:
Certificate name/subject: XILINX Vivado Tooling Certificate
Certification body: TUV SUD
Certificate number: Z10 16 11 84605 004

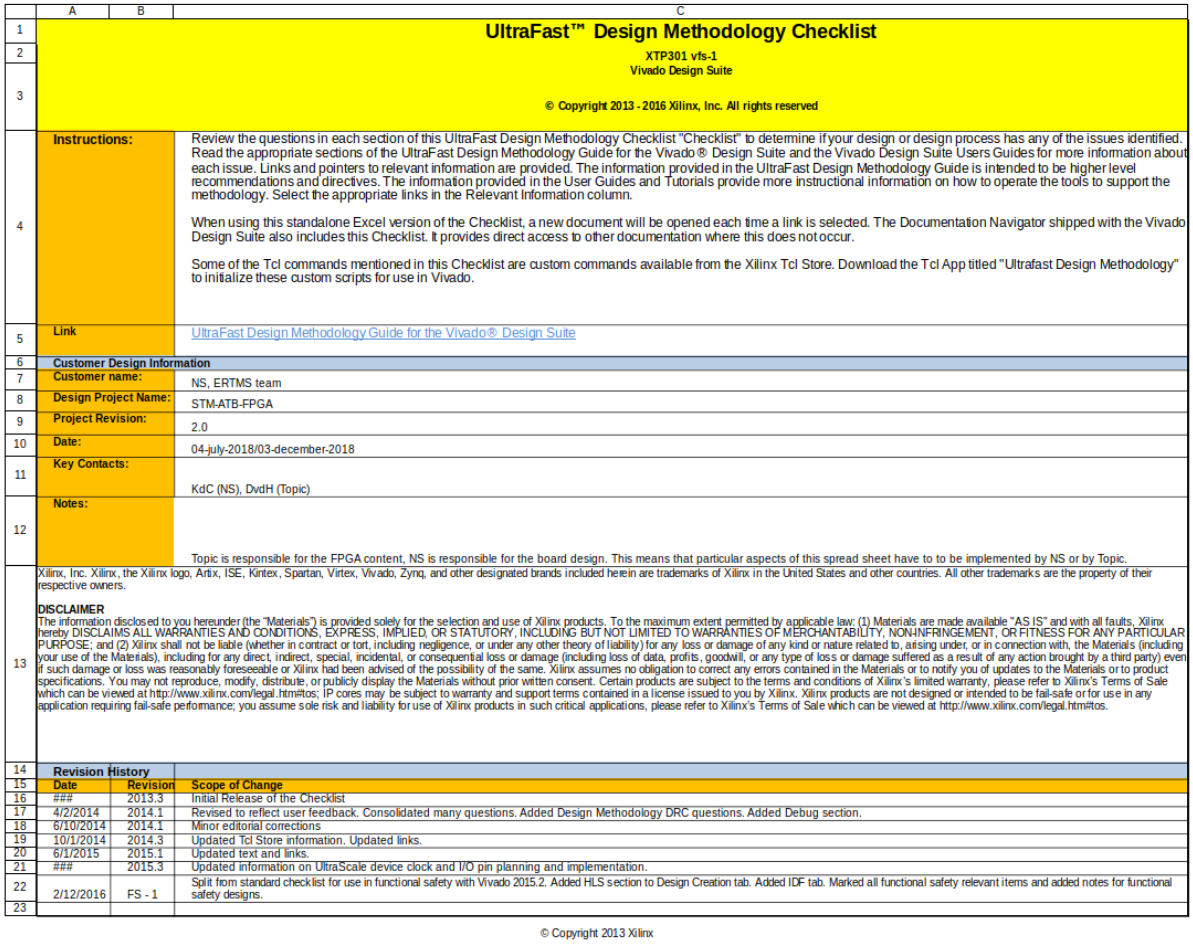
The FPGA design complies to all conditions of use imposed by STMA-63019 - Xilinx Vivado tooling certificate: Certificate name/subject: XILINX Vivado Tooli.... See IEC610508-7_F2.xlsx.

For proper usage of the device the "Xilinx Functional Safety Guide" [UG1187] and "'Isolation Design Flow for Xilinx 7 Series FPGAs or Zynq-7000 AP SoCs" [XAPP1222] were followed. Also the "Safety Design Methodology Checklist" [XTP301] was used.The device failure rate was calculated with the method "Calculating Artix-7 Base Failure rates for Functional Safety Applications" [XAPP1310].

Document	Reference
Device Reliability Report	UG116
Xilinx Functional Safety Guide	UG1187
Safety Design Methodology Checklist	XTP301
Isolation Design Flow for Xilinx 7 Series FPGAs or Zynq-7000 AP SoCs (Vivado Tools)	XAPP1222

Calculating Artix-7 Base Failure rates for Functional Safety Applications	XAPP131

The Safety Design Methodology Checklist [XTP301] provided by Xilinx was used. Only the title page is displayed here, but the full report can be found on SVN.



UltraFast™ Design Methodology Checklist

XTP301 vfs-1
Vivado Design Suite

Instructions:	Review the questions in each section of this UltraFast Design Methodology Checklist "Checklist" to determine if your design or design process has any of the issues identified. Read the appropriate sections of the UltraFast Design Methodology Guide for the Vivado® Design Suite and the Vivado Design Suite Users Guides for more information about each issue. Links and pointers to relevant information are provided. The information provided in the UltraFast Design Methodology Guide is intended to be higher level recommendations and directives. The information provided in the User Guides and Tutorials provide more instructional information on how to operate the tools to support the methodology. Select the appropriate links in the Relevant Information column. When using this standalone Excel version of the Checklist, a new document will be opened each time a link is selected. The Documentation Navigator shipped with the Vivado Design Suite also includes this Checklist. It provides direct access to other documentation where this does not occur. Some of the Tcl commands mentioned in this Checklist are custom commands available from the Xilinx Tcl Store. Download the Tcl App titled "Ultrafast Design Methodology" to initialize these custom scripts for use in Vivado.
Link	UltraFast Design Methodology Guide for the Vivado® Design Suite

Customer Design Information	
Customer name:	NS, ERTMS team
Design Project Name:	STM-ATB-FPGA
Project Revision:	2.0
Date:	04-july-2018/03-december-2018
Key Contacts:	KdC (NS), DvdH (Topic)
Notes:	Topic is responsible for the FPGA content, NS is responsible for the board design. This means that particular aspects of this spread sheet have to to be implemented by NS or by Topic.

Revision History

Date	Revision	Scope of Change
###	2013.3	Initial Release of the Checklist
4/2/2014	2014.1	Revised to reflect user feedback. Consolidated many questions. Added Design Methodology DRC questions. Added Debug section.
6/10/2014	2014.1	Minor editorial corrections
10/1/2014	2014.3	Updated Tcl Store information. Updated links.
6/1/2015	2015.1	Updated text and links.
###	2015.3	Updated information on UltraScale device clock and I/O pin planning and implementation.
2/12/2016	FS - 1	Split from standard checklist for use in functional safety with Vivado 2015.2. Added HLS section to Design Creation tab. Added IDF tab. Marked all functional safety relevant items and added notes for functional safety designs.

The filled in spreadsheet can be found on SVN
(D. Develop/Ph6/D6.2 SW Designs/D6.2.9 IO Channels/Verification/STM-ATB-xtp301_safety-design-methodology-checklist_ano.xlsx).
The results from the scripts in this document can also be found on SVN:
(D. Develop/Ph6/D6.2 SW Designs/D6.2.9 IO Channels/Verification/STM_ATB_Top_reports.zip).

Xilinx has provided a tool to generate a schematic review checklist [XMP277] which can be found on SVN (D. Develop/0.0 comp doc/FPGA/xmp277-7series-schematic-review-recommendations.zip).
The schematic review results are stored on SVN (D. Develop/Ph6/D6.1 HW Designs/D6.1.5 SAP Board/D6.1.5.4 C2-sample/7_Series_Schematic_Review_Recommendations.xlsm).