中核控制系统工程有限公司
CHINA NUCLEAR CONTROL SYSTEM ENGINEERING CO., LTD.

CNCS

Software Tool Qualification in FPGA-based Safety I&C System

Lin Shuqian

China Nuclear Control System Engineering Co.,Ltd

Outline

1. Preface
2. Workflow of COTS tool qualification
3. Identify the software tool used in 8000N platform
4. Tool qualification cases

Outline

1. Preface
2. Workflow of COTS tool qualification
3. Identify the software tool used in 8000N platform
4. Tool qualification cases

1.Preface

• The use of appropriate software tools can increase the integrity of the software development process, and have economic benefits as they can reduce the time and human effort required to produce software, but the use of tool may introduce new error in the software. So before using the software tool, we must make sure the tool is safety and reliability.

• From another standpoint, the software tool can be approved for use in safety-related applications:

- If critical characteristics of the tool cannot be verified, then the tool must be designed and manufactured under a QA program.
- If critical characteristics of the tool can be verified, then the tool may be designed and manufactured as a CGI and then commercially dedicated under a QA program. (ISG-06)

In conclusion, research on tool evaluation and qualification are very important and necessary.

Outline

1. Preface
2. Workflow of COTS tool qualification
3. Identify the software tool used in 8000N platform
4. Tool qualification cases

2.Workflow of COTS tool qualification

• There is currently no specific and detailed standard and commonly accepted practice in the nuclear industry that address the software tool development, evaluation and qualification.

•So how can we do the research of COTS tool qualification?

•Task 1: Survey the related standards and guidance

•Task 2: Analysis the demands from the related standards and guidance

•Task 3: Conclude the workflow

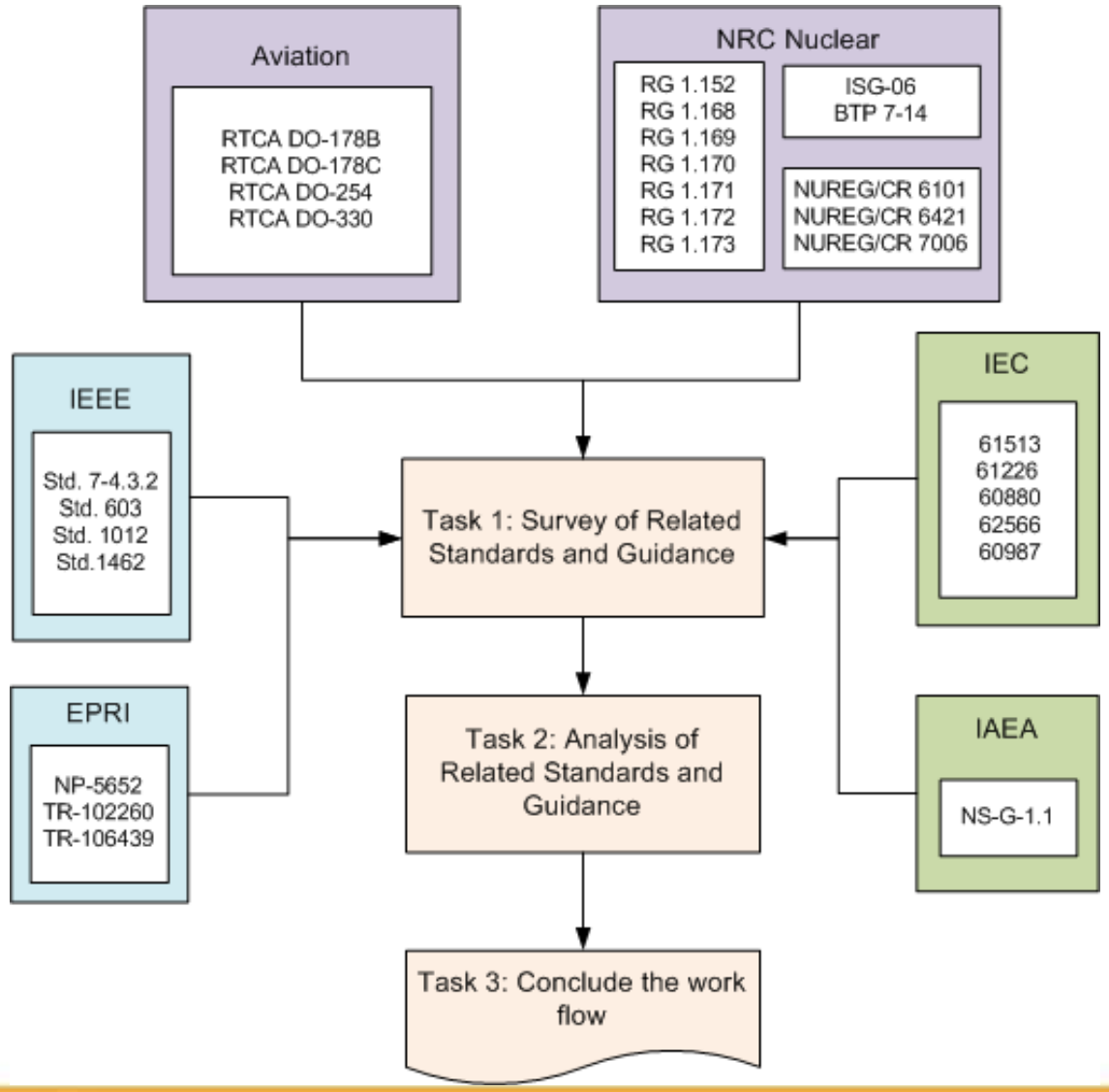
2.Workflow of COTS tool qualification

Task 1: Survey the related standards and guidance

•There are some standards and guidance in nuclear industry give a little hints about COTS tool qualification like that:
IEEE: std.7-4.3.2, std.1012, std.14102
IEC: 60880
EPRI: NP-5652, NP-6406, TR-106439, TR-102260
RG 1.152, ISG-06,BTP7-14,NUREG/CR-6421 etc

•There are several reference standards in similar industry such as aviation ,like that:
•DO-254, DO-178B&C,DO-330

Task 1: Survey the related standards and guidance



2.Workflow of COTS tool qualification

Task 2: Analysis the demands from the related standards and guidance

Standards	Target	Content	Note
EPRI NP-5652 (EPRI TR-102260)	Commercial Grade Item (CGI)	Method 1-4	Focus on hardware equipments
EPRI TR-106439	CGI digital equipment	Process for accepting CGIs	Focus on software-based equipments
NUREG/CR-6421	COTS software	Processes for each safety category	Detailed acceptance criteria
IEEE 7-4.3.2 (ISG-06)	Commercial computer	Guidance for the dedication	Just a general description
IEC 60880 (Chapter 14)	Software tool	Criterion for tool qualification	Not detail process
DO-330	Software tool	Process for qualification and development	Focus on COTS tool qualification

2.Workflow of COTS tool qualification

Task 3: Conclude the workflow

•After analysis and conclusion, the COTS tool used in safety-related application must be considered as configuration item, and placed under configuration control.

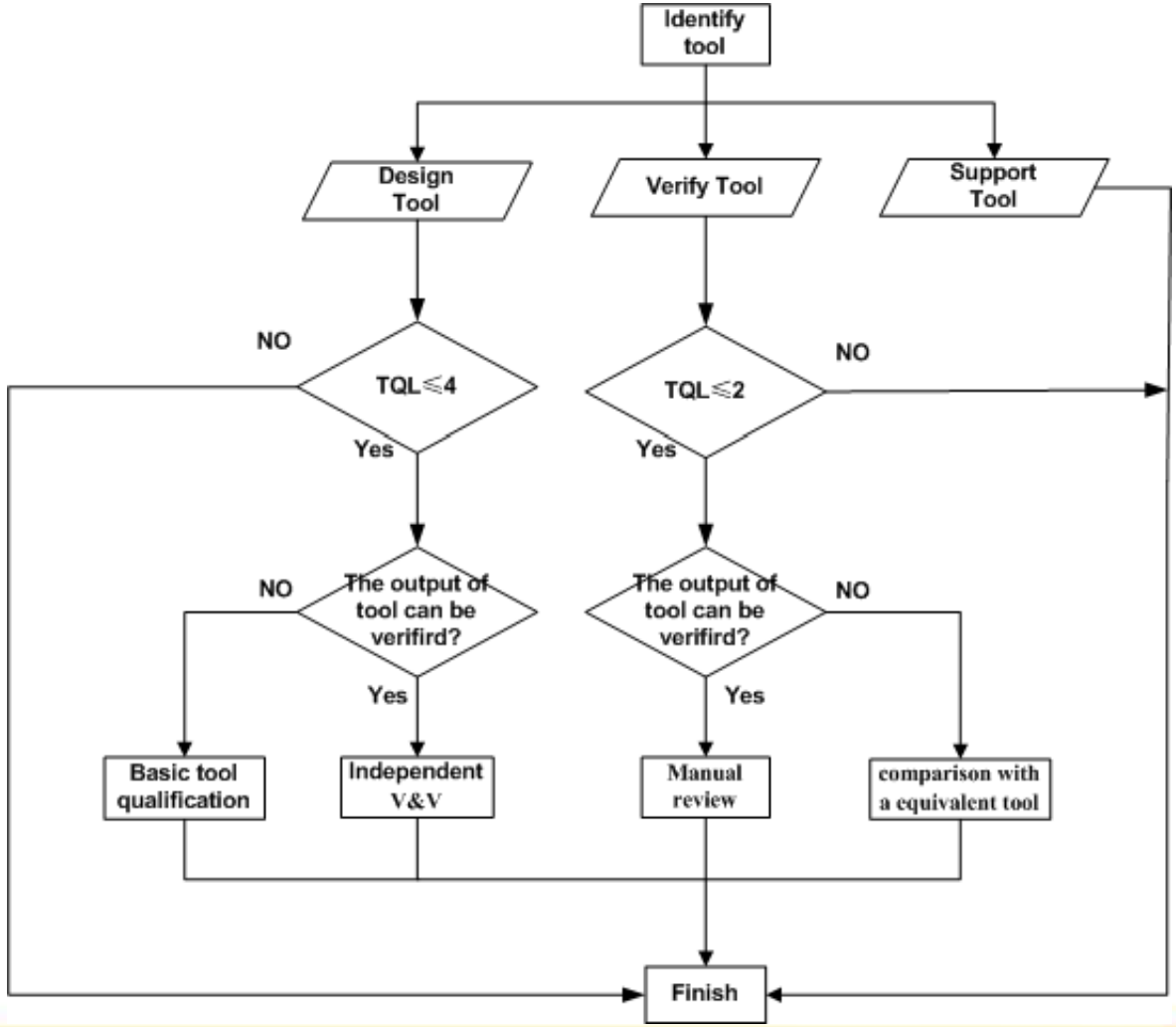
•And the software tool can be divided into five tool qualification levels, see the table below:

Software level	Design tool	V&V tool	Support tool
A	TQL-1	TQL-2	TQL-4
B	TQL-2	TQL-3	TQL-5
C	TQL-3	TQL-4	TQL-5
D	TQL-4	TQL-5	TQL-5

2.Workflow of COTS tool qualification

Task 3: Conclude the workflow (continue)

The detail workflow is as the left:
First, we need to identify the three categories of software tool;
And then according to the tool qualification level(TQL) to decide go which branch Path.

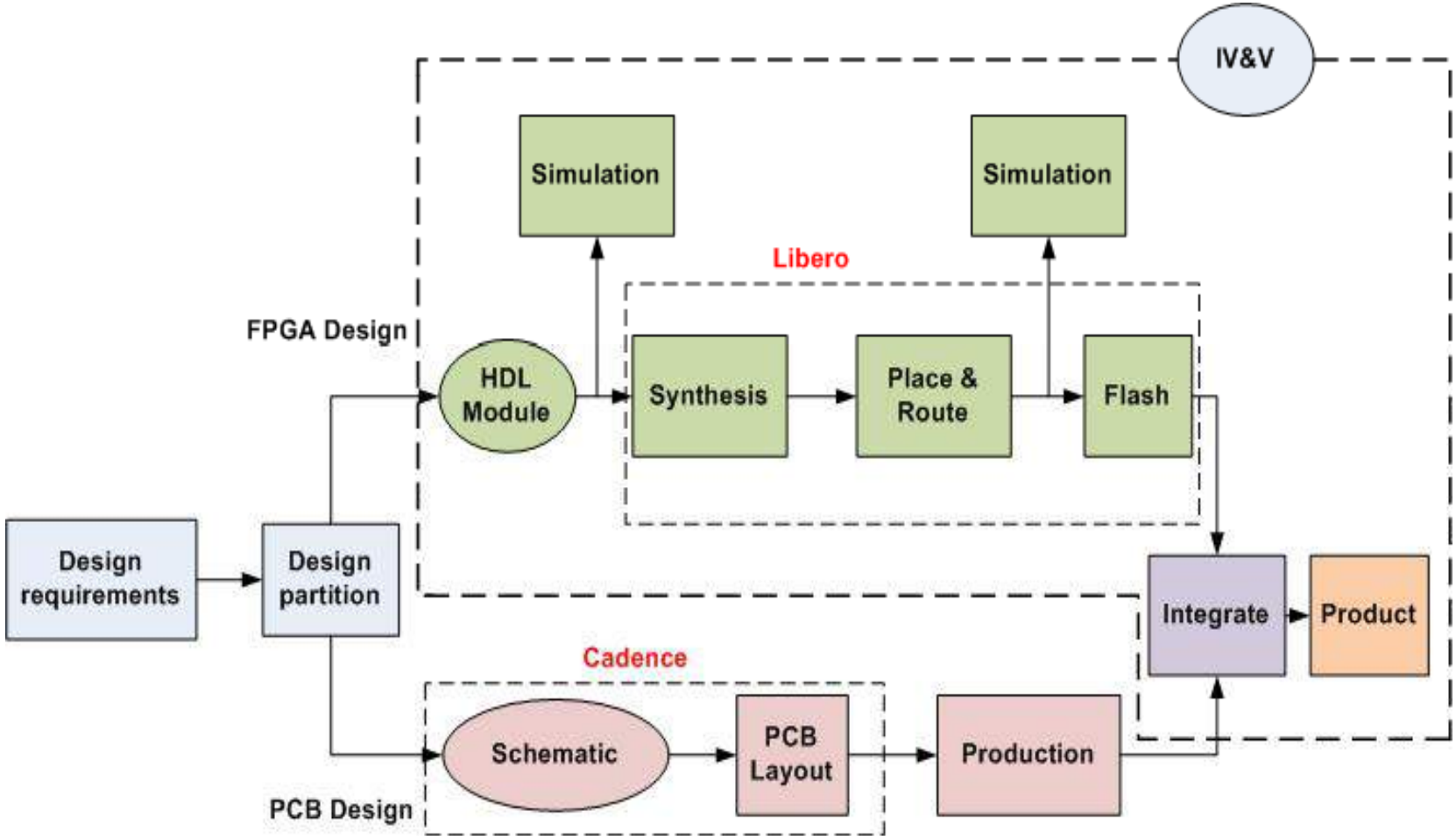


Outline

1. Preface
2. Workflow of COTS tool qualification
3. Identify the software tool used in 8000N platform
4. Tool qualification cases

3. Identify the software tool used in 8000N platform

- The general FPGA development flow is as below:



3. Identify the software tool used in 8000N platform

In the whole development process, the software tools used can be placed into three categories:

- Design Tool
  - FPGA Design tool: RTL editor, Synplify, FloorPlan, FlashPro
  - PCB Design tool: OrCAD, Allegro
- IV&V tool: Leda, VCS MX, Formality .etc
- Support Tool: SVN, V&V Solution, DOORS

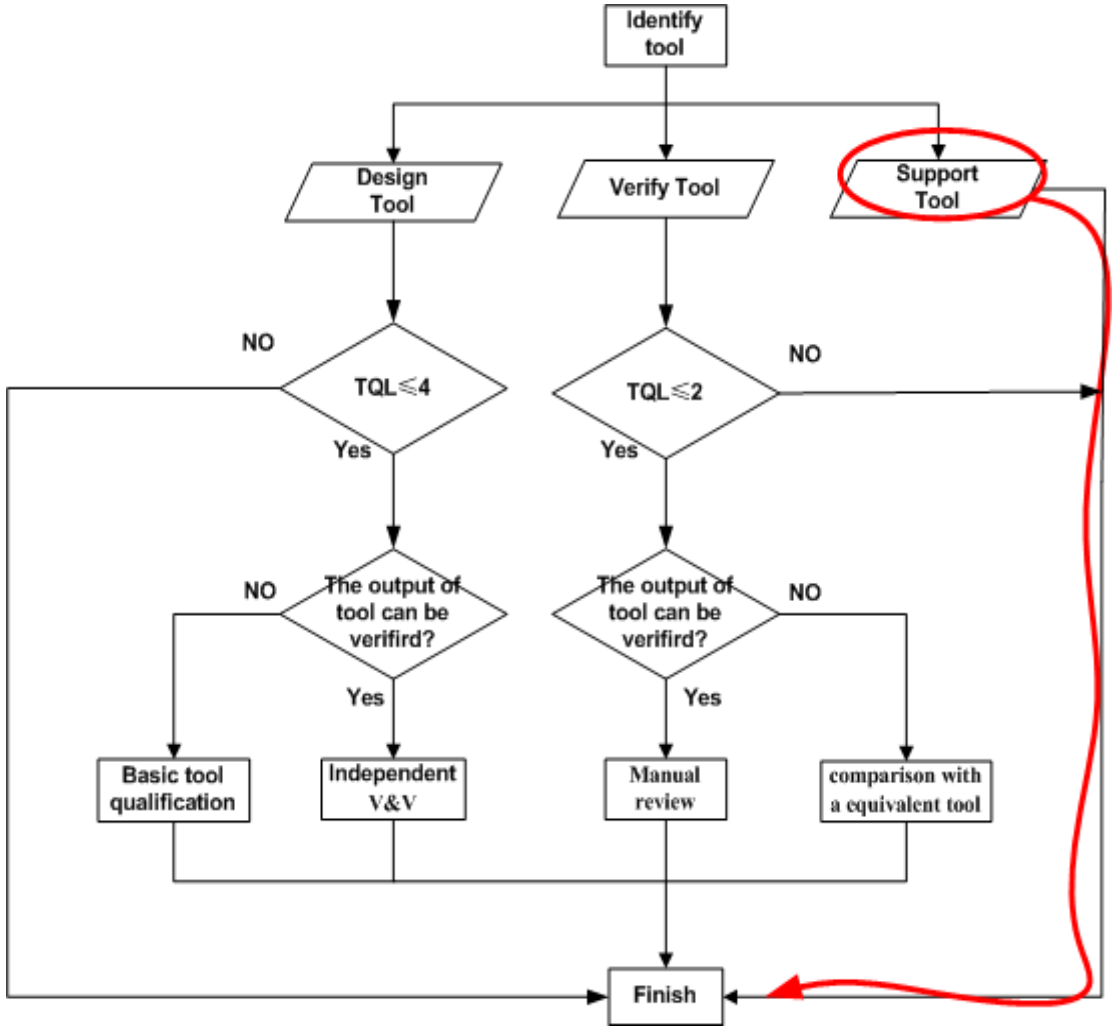
Outline

1. Preface
2. Workflow of COTS tool qualification
3. Identify the software tool used in 8000N platform
4. Tool qualification cases

4.Tool qualification case 1

•Case 1
IBM Rational DOORS

•It is a requirements management application for optimizing requirements communication, collaboration and verification throughout your organization and supply chain.
•We plan to use DOORS to capture, trace, analyze and manage requirements.

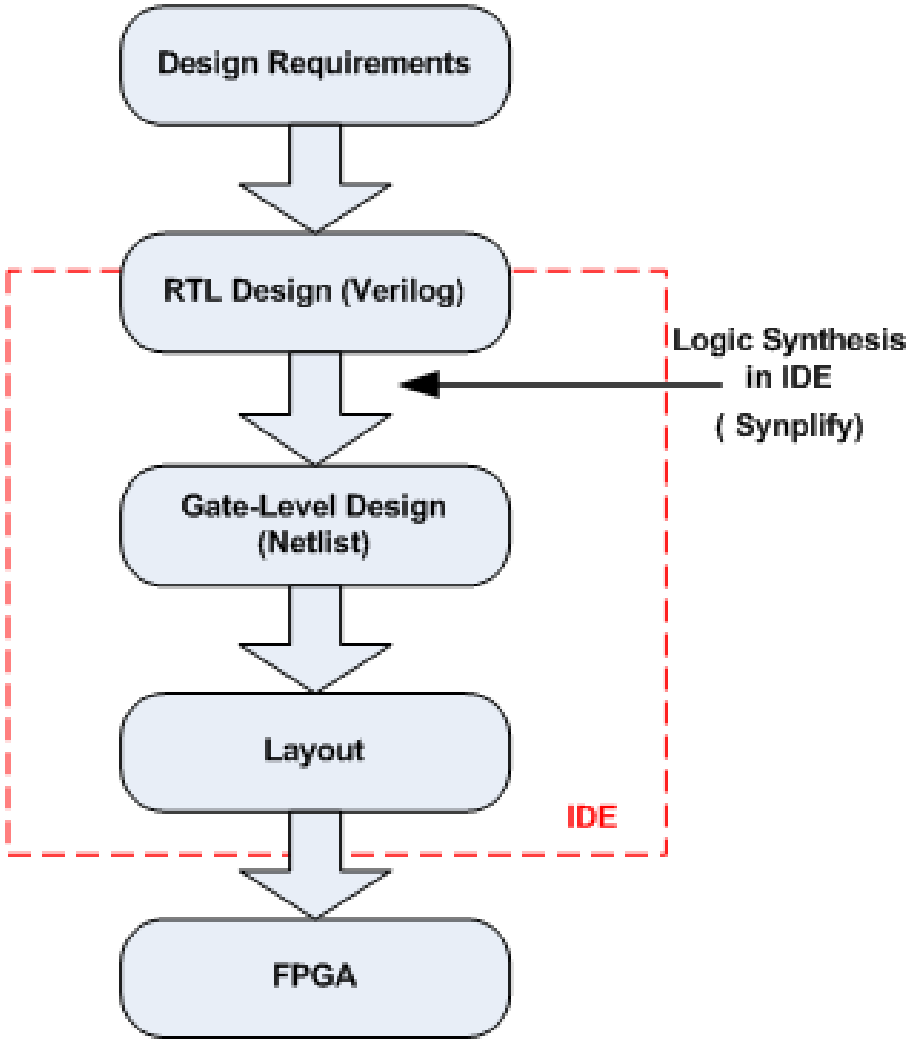


4.Tool qualification case 2

•Case 2 Synplify

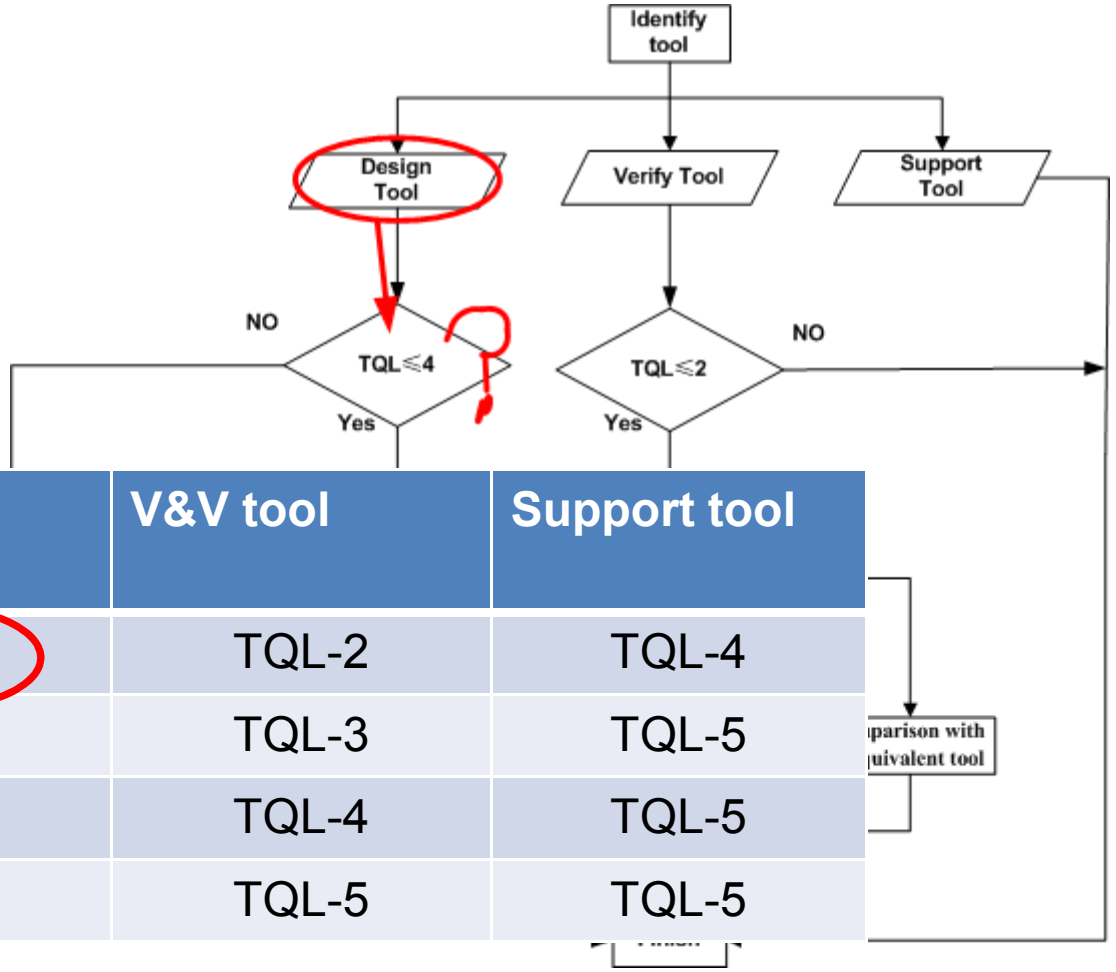
•Synplify is a 3rd party synthesis tool used in Libero, produced by Synplicity. Synplicity is a market leading supplier of FPGA synthesis tools and have been the Actel preferred synthesis tool since 2003.

• The purpose of the synthesis tool is to map the RTL description into netlist in the FPGA.



4.Tool qualification case 2

•According to the workflow, is the synthesis tool qualification level equal and small four?



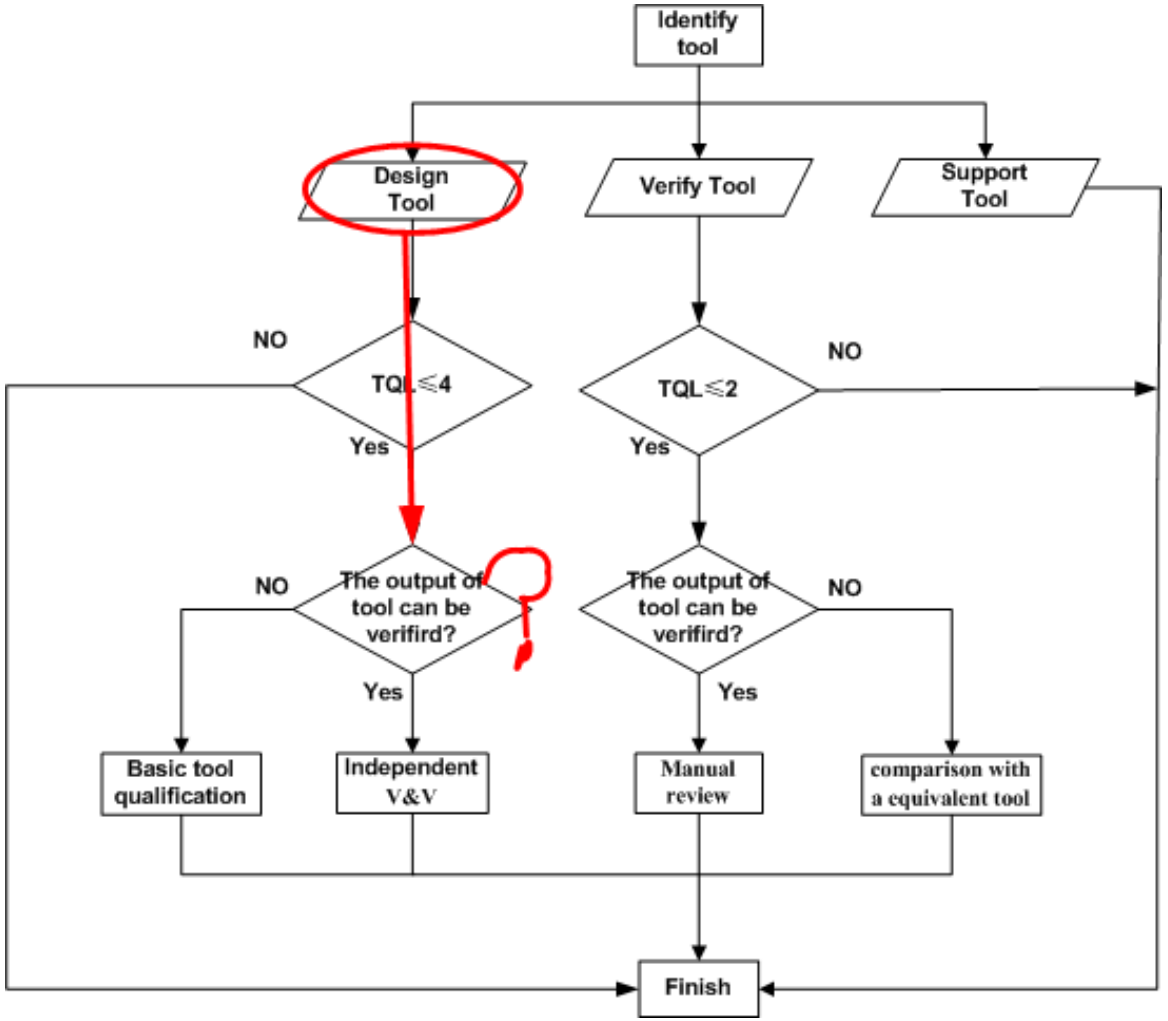
Software level	Design tool	V&V tool	Support tool
A	TQL-1	TQL-2	TQL-4
B	TQL-2	TQL-3	TQL-5
C	TQL-3	TQL-4	TQL-5
D	TQL-4	TQL-5	TQL-5

4.Tool qualification case 2

•The second judgement: Can the output of tool be verified?

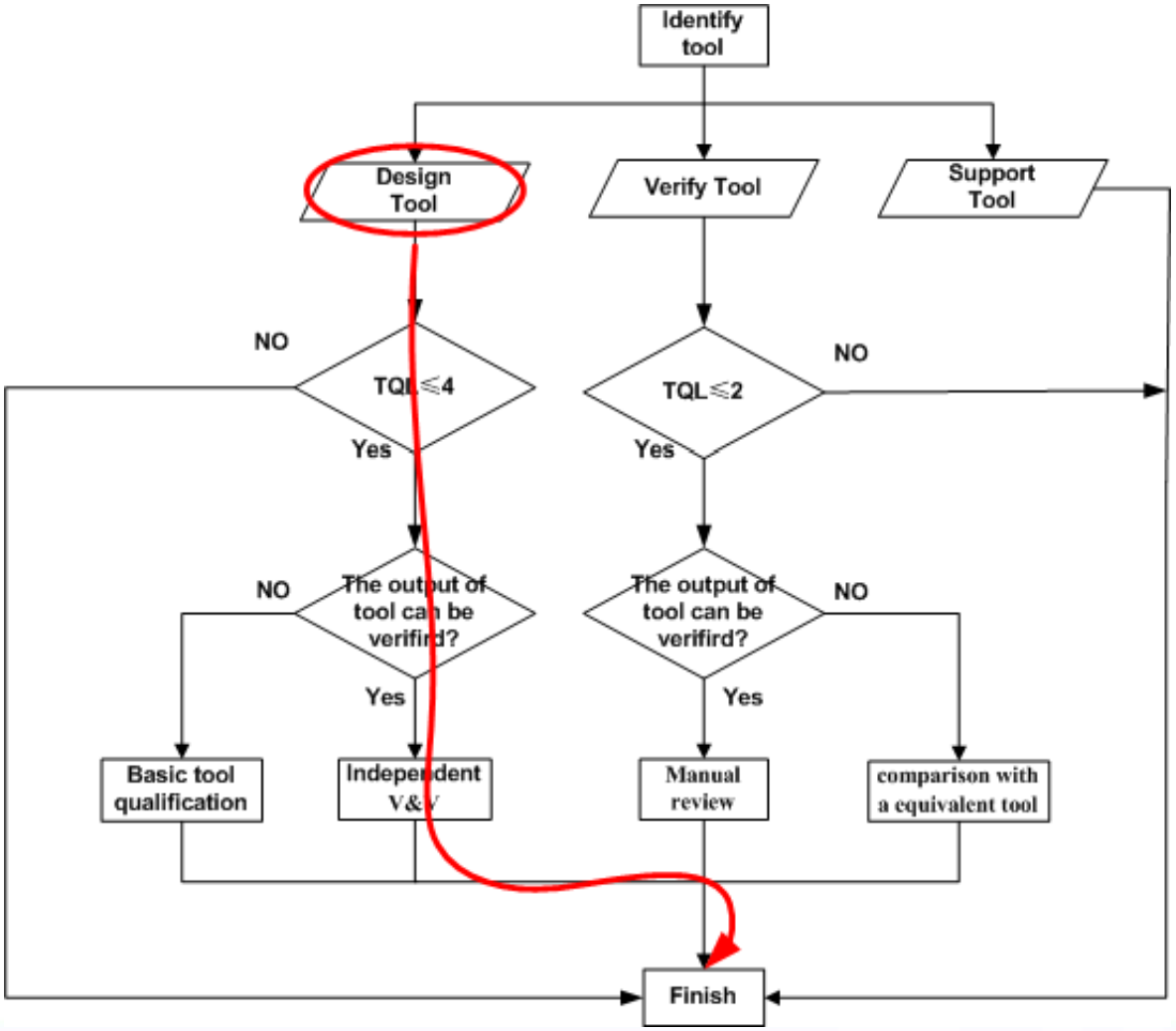
•If no, the tool must complete basic qualification;

•If yes, the software tool will be verified by V&V activities.



4.Tool qualification case 2

Then for Synplify ,we could use logic equivalence checking to verify that for a special input, the output always shows the same behavior with the input.



Summary

FPGA is receiving international attention as an alternative platform of digital I&Cs in NPP.

We should do the COTS SW tool qualification to demonstrate correctness and safety of commercial software used, such as IDEs, according to international standards.

COTS SW tool qualification involves an in-depth analysis on the target's functionality and the techniques used to verify the functionality.

Our target is build an entire work procedure of COTS tool qualification base on current standards and develop customized solution for special tools.

Thank you for your attention!
Questions & Comments?