Formality®
Formality Ultra
Functional Safety Manual

March 2018, Revision 1.4

SYNOPSYS®

Copyright and Proprietary Information Notice

Destination Control Statement

All technical data contained in this publication is subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

SYNOPSYS, INC., AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

Synopsys and certain Synopsys product names are trademarks of Synopsys, as set forth at https://www.synopsys.com/company/legal/trademarks-brands.html.
All other product or company names may be trademarks of their respective owners.

Third-Party Links

Any links to third-party websites included in this document are for your convenience only. Synopsys does not endorse and is not responsible for such websites and their practices, including privacy practices, availability, and content.

Synopsys, Inc.
690 E. Middlefield Road
Mountain View, CA, 94043
www.synopsys.com

Document Control

Revision history

Version	Description	Date
1.0	First release of the document submitted for review.	12-Jan-2018
1.1	Added revision history, fixed template issues; Added Appendix B	06-Feb-2018
1.2	Fixed boilerplate changes from general feedback.	01-Mar-2018
1.3	Updated content based on certification review	09-Mar-2018
1.4	Added AoU-FM-005	13-Mar-2018

Contents

1 Customer Support

This section describes the customer support that is available through the Synopsys SolvNet® customer support website or by contacting the Synopsys support center.

Accessing SolvNet

The SolvNet support site includes an electronic knowledge base of technical articles and answers to frequently asked questions about Synopsys tools. The site also gives you access to a wide range of Synopsys online services, which include downloading software, viewing documentation, and entering a call to the Support Center.

To access the SolvNet site:

1. Go to the web page at https://solvnet.synopsys.com.
2. If prompted, enter your user name and password. (If you do not have a Synopsys user name and password, follow the instructions to register.)

If you need help using the site, click **Help** on the menu bar.

Contacting Synopsys Support

If you have problems, questions, or suggestions, you can contact the Synopsys support center in the following ways:

- Go to the Synopsys Global Support Centers site on synopsys.com. There you can find e-mail addresses and telephone numbers for Synopsys support centers throughout the world.
- Go to either the Synopsys SolvNet site or the Synopsys Global Support Centers site and open a case online (Synopsys user name and password required).

2
Scope of This Document

This section describes the scope of this document and defines terms used in this document.

Using This Document

The *Formality Functional Safety Manual* describes the proper use of the Formality tool in safety-related applications according to the ISO 26262 standard, and is intended to confirm the compliance of the Formality tool to the standard when used in the context of a tool chain.

The family of Synopsys formal equivalence checking tools comprise of Formality and Formality Ultra and these tools are covered in this document. Both of these products are primarily referenced in this document as the Formality tool. Section 6 specifically lists out which of the formal equivalence products apply to that particular use case.

During the development from RTL to final Netlist, the design undergoes changes due to optimizations throughout the flow. The optimized design still be functionally equivalent to the original version of the design through each stage of optimization. The *Formality* tool is an equivalence checker that enables the user to detect any unexpected differences that might have been introduced into a design during development. It uses a formal verification comparison engine to prove or disprove the equivalence of the two specified designs and presents any differences for further detailed analysis.

Formality Ultra allows the user to interactively generate a netlist. It also uses a formal verification comparison engine to prove or disprove the equivalence of the generated netlist with ECO RTL designs and presents any differences for further detailed analysis.

Section 3 describes an overview of the ISO 26262-8, clause 11 and the approach adopted by Synopsys to comply with the requirements of the standard. Section 4 defines the general information such as where to find the latest documentation and installation requirements regarding the use of the Formality tool as a software tool in the development of safety-related applications. Section 5 shows the high-level overview of the tool chain that this product belongs to. Section 6 details the safety-related requirements for safety-qualified use cases of the Formality tool. Section 7 lists the known limitations of the use cases.

Specific documentation for performing design and analysis as part of an ISO 26262 compliant flow is provided in Section 3, Section 5, Section 6, Appendix A, and Appendix B of this document, the *Formality Functional Safety Manual*.

Terms and Definitions

Term	Definition
AoU	Assumption of Use. An action that is assumed and required to be taken by the user of a software tool.
ASIL	Automotive Safety Integrity Level. This is a risk classification scheme defined by the standard ISO 26262. The standard identifies four levels: ASIL A, ASIL B, ASIL C, and ASIL D. ASIL D dictates the highest integrity requirements on a product and ASIL A dictates the lowest.
BIST	Built In Self Test is a mechanism used in a machine to test itself and thereby reduce dependance on external pattern generating equipment.
Component	A part of an electronic system that implements a function in a vehicle. See also Part 1 of the standard ISO 26262 for the definition. The standard also refers to elements and items, but for the *Formality Functional Safety Manual*, there is no difference.
CoU	Condition of Use. A condition of the design, software tool, design environment, or situation that is assumed and required to be fulfilled by the user.
CRM	Customer Relationship Management. Internal Synopsys database that manages customer STARs.
Defect	Product nonconformance.
.db	A Synopys internal binary file format for storing library and design data.
ECO	A modification made in the design during an intermediate stage of implementation to achieve a timing or a functional change is termed as an Electronic Change Order.
Error	An error is a discrepancy between the actual and the specified or theoretically correct operation of an element. The root causes of an error can be manifold. In this document, the focus is on errors that are introduced or left undetected in a design, due to the malfunction in a software tool (e.g. generation of bad logic by a logic synthesis tool, failure of a static timing analysis tool to detect a timing violation).

Term	Definition
Fault	An abnormal condition that can cause an element or item to fail.
Fault analysis	An analysis that determines the behavior of a system when a fault is introduced.
FMEA	Failure Mode and Effects Analysis. An analysis that looks at different parts of a system, identifies ways the parts could fail, and determines the causes and effects of these potential failures.
Implementation Design	The version of the design that is compared with the reference design in the Formality tool. After verifying successfully, the implementation design can be used as a reference design for subsequent verifications.
Reference Design	The version of the design that is termed as “golden” in the Formality tool. The implementation design is compared with the reference design.
RTL	The register Transfer Level. A level of design abstraction where data is moved from register to register.
Software / software tool	The Formality tool.
Software tool criteria evaluation	Analysis according to ISO 26262 to determine the required TCL of a software tool.
Software tool qualification	Means to create evidence, that a software tool with low or medium TCL is suitable to be used in the development of safety related products according to ISO 26262.
SolvNet	Synopsys customer support site.
Standard	In this document, refers to *ISO 26262 Road Vehicles – Functional Safety*, 2011 and 2018 versions.
SVF	A automated setup verification file (SVF) that enables the Formality tool to process design changes caused by other tools used in the design flow and store data for use during the matching step that follows.

Term	Definition
STAR	Synopsys Technical Action Request. A STAR documents and tracks a product Bug or Enhancement request (called a B-STAR or an E-STAR, respectively). It is stored in the Synopsys CRM database. Only Synopsys employees can access the CRM database. However, limited STAR information is available from SolvNet for customers who are associated with the user site of a STAR. Customer contacts are notified automatically when a STAR is filed or when its status changes.
TCL	Tool confidence level, as defined by ISO 26262-8, clause 11. Note: The TCL of a software tool does not necessarily indicate whether the tool may malfunction or not. The TCL defines the confidence level that an error in the safety-related design, which is introduced or left undetected by the software tool, can be prevented or detected in subsequent steps of the development flow, before the erroneous safety-related design is released.
TD	Tool error detection, as defined in ISO 26262-8, clause 11.
TI	Tool impact, as defined in ISO 26262-8, clause 11.
Use case	A use case is a specific way of using a software tool, that can be characterized by: - a limited set of tool functions and features that are used; - a set of restrictions and constraints that are regarded while using the tool; and - a specific goal to be achieved or output to be generated by using the software tool Use cases may be associated with different steps or phases in the design process, or they may describe alternative ways of using the tool for a specific design step.

3 Confidence in the Use of Software Tools According to ISO 26262-8, Clause 11

This section provides an overview of the ISO 26262-8, clause 11. It then describes the approach adopted by Synopsys to comply with the requirements of the standard, and how this is mapped to activities performed by Synopsys and the end user of the Synopsys tools.

Overview of ISO 26262-8, Clause 11

Synopsys EDA software tools contribute significantly to the design specification, implementation, integration, verification and validation of electrical and electronic (E/E) systems and components. If these E/E systems and components are used as part of a safety-related automotive product, an error in these systems or components could have severe consequences on functional safety. Such an error may arise as a result of unforeseen operating conditions or due to a fault introduced during product development, which in turn may be caused by a software tool malfunction. ISO 26262-8, clause 11 (Confidence in the Use of Software Tools) addresses this issue and specifies requirements and methods which aim to minimize the risk of faults in the developed product due to malfunctions of a software tool affecting the product's functional safety.

According to ISO 26262, to determine the required level of confidence in a software tool that is used in the development of a safety-related automotive product, the following criteria are evaluated:

- The possibility that the malfunctioning software tool and its corresponding erroneous output can introduce or fail to detect errors in a safety-related element being developed.
- The confidence in preventing or detecting such errors in its corresponding output.

This procedure is called Software Tool Criteria Evaluation, and it must be performed for all software tools that are involved in the development of a safety-related element, resulting in a required Tool Confidence Level (TCL) for each software tool.

If the software tool criteria evaluation determines that a medium or high TCL is required, then appropriate Software Qualification methods must be applied, effectively reducing the risk of a critical software tool error. The choice of software qualification methods depends on the required TCL and the maximum ASIL of all the safety requirements allocated to the element developed using the software tool. However, if the software tool criteria evaluation determines that only a low TCL is required, then there is no need to apply such software qualification methods.

The software tool criteria evaluation and software tool qualification flow is summarized in Figure 1.

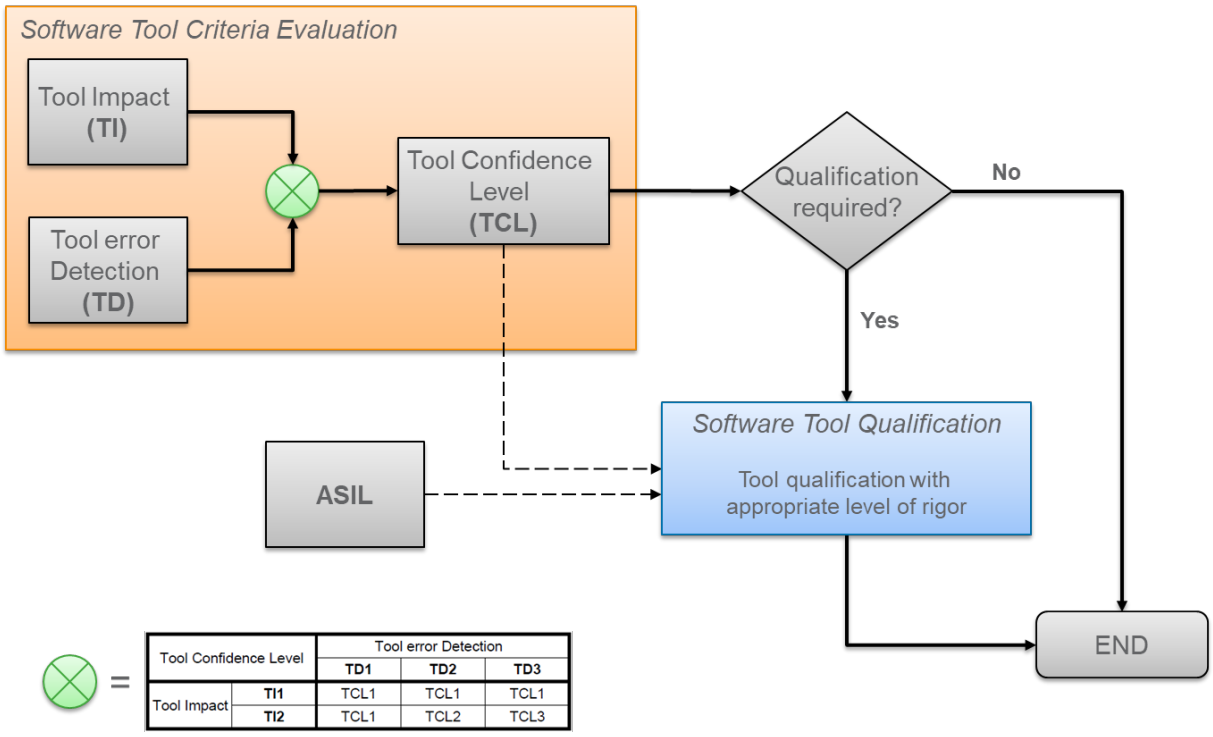


Figure 1: Software tool criteria evaluation and software tool qualification flow

Work Split between Synopsys and Tool Users

A software tool criteria evaluation must always be performed in the development environment of the final tool user, and in the context of the actual product development. It is in this context, where potential tool malfunctions, their effect on the safety-related product, and the effectiveness of prevention and detection measures must be analyzed.

However, the tool vendor can support the tool user by performing a software tool criteria evaluation (and, if required, a software tool qualification) on their own, based on assumed tool use cases and an assumed development environment. If the assumptions made by the tool vendor match the actual situation at the tool user, then the user can take over the evaluation (and qualification) results from the tool vendor. Besides significantly reducing the effort for the tool user, this approach can also result in a better quality for the software tool criteria evaluation and qualification, since the tool vendor typically has a more detailed understanding of the inner working and possible malfunctions of the software tool.

Synopsys has adopted exactly this approach, which is summarized in Figure 2.

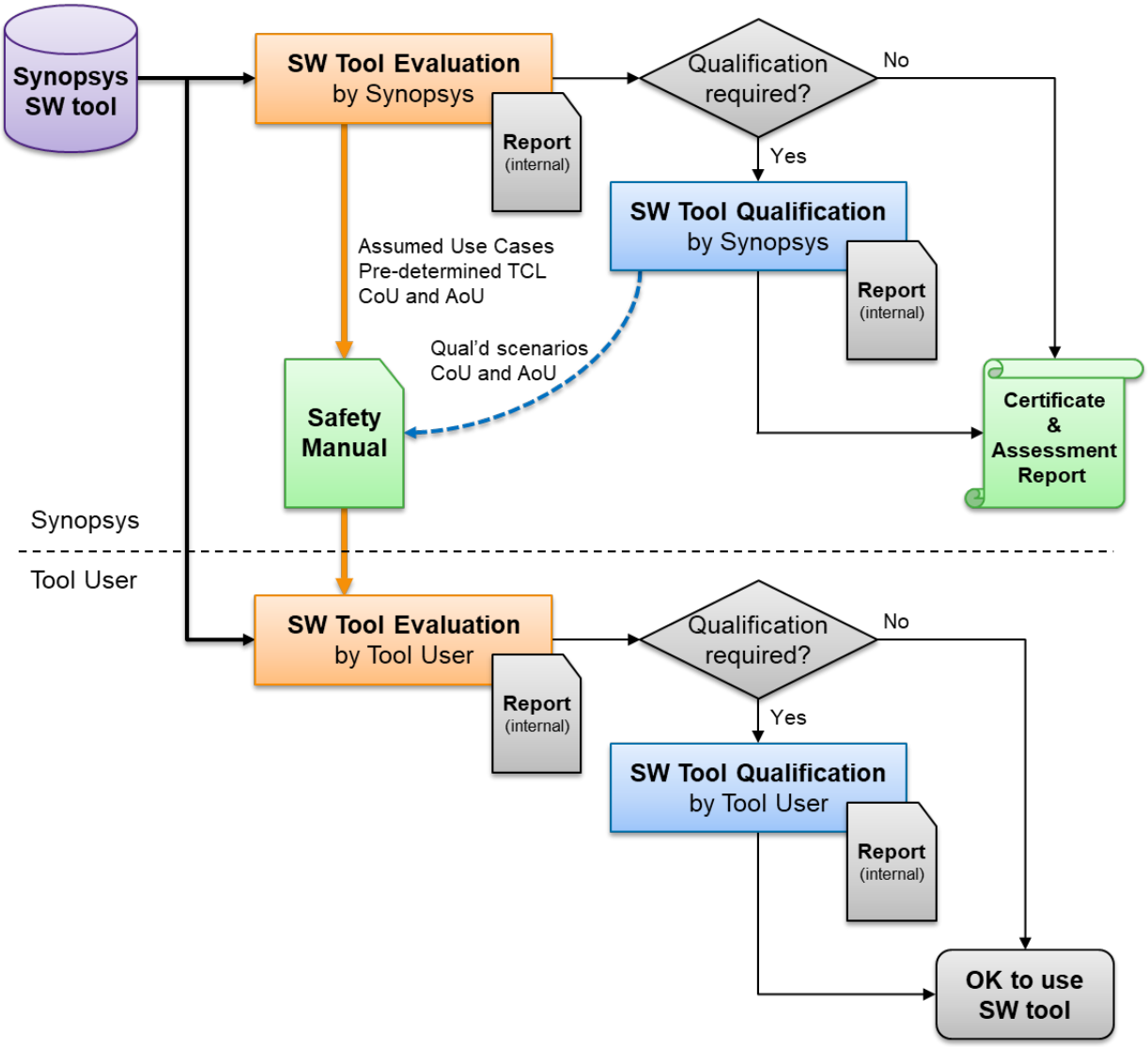


Figure 2: Work Split between Synopsys and Tool Users

Synopsys performs the following activities:

1. Software tool criteria evaluation
   - Identification of possible **use cases** for the software tool, together with required **inputs** and expected **outputs**
   - Specification of **conditions of use (CoU)** for each use case, related to the development environment in which the tool is assumed to be deployed, including tool usage procedures and constraints
   - Analysis of potential software tool **malfunctions**, and their effect on a safety-related product that is developed with this tool
   - Analysis of **prevention** and **detection measures** internal to the software tool, to avoid tool malfunctions, or to control and mitigate their effects
   - Specification of **assumptions of use (AoU)**, which are additional prevention and detection measures assumed to be performed by the end user of the tool

- Estimation of the **Tool Impact (TI)** for each malfunction, and the probability of **Tool error Detection (TD)** by the prevention and detection mechanisms (including assumptions of use)
- Determination of the required **Tool Confidence Level (TCL)** for each software tool malfunction, based on TI and TD
- Determination of the maximum TCL from all software tool malfunctions related to a use case. This is called the **pre-determined TCL** for the software tool use case
- Summary of the results in a software tool criteria evaluation report

2. Software tool qualification
   - If the pre-determined TCL indicates, that a medium (TCL2) or high (TCL3) tool confidence level is required for the software tool, then Synopsys may decide to perform a software tool qualification
   - The specific methods applied for tool qualification can vary for different tools and use cases, and they may include an evaluation of the software tool development process, the validation of the complete software tool, the validation of critical tool malfunctions with insufficient prevention and detection measures, or other methods
   - Summary of the qualification methods, procedures and results in a software tool qualification report

3. Safety manual for the software tool
   - The *Formality Functional Safety Manual* (this document) is an important deliverable to the tool users, as it includes all end user-relevant information from the Synopsys software tool criteria evaluation and qualification
   - Software tool criteria evaluation related information, documented in Section 6, includes:
     - Description of software tool use cases
     - Description of the required inputs and expected outputs for each use case
     - Specification of conditions of use (CoU – conditions of the design, software tool, design environment, or situation that are assumed and required to be fulfilled by the user) for each use case
     - Specification of assumptions of use (AoU – actions that are assumed and required to be taken by the user of a software tool) for each use case
     - Pre-determined TCL for each use case
   - Software tool qualification related information (not required for this Formality and therefore not included in this safety manual)
     - Description of the scope of the software tool qualification, including malfunctions and scenarios covered by the qualification
     - Specification of additional conditions of use (CoU) derived from the software tool qualification
     - Specification of additional assumptions of use (AoU) derived from the software tool qualification
   - Other information included in this safety manual
     - General information about the software tool needed by the tool user (see Appendix A)
     - Known limitations of the software tool, related to the described use cases as documented in Section 7

4. Certification and assessment report
   - Synopsys may decide to perform a functional safety assessment, to confirm the correctness, completeness and ISO 26262 conformance of the performed software tool criteria evaluation and qualification
   - Synopsys may also decide to achieve certification from an accredited third-party certification body, in addition to the functional safety assessment
   - The results of these activities are summarized in a functional safety assessment report and a certificate which can be viewed at exida Certificate for ISO 26262 Compliance

If the tool user wants to benefit from the work done by Synopsys, then according to the Figure 2 above, the user shall perform the following activities for each software tool:

1. Software tool criteria evaluation
   - Review and verify that the software tool criteria evaluation (and qualification) performed by Synopsys, as documented in the tool‘s Functional Safety Manual, matches the actual situation of the user’s product development process
     - Verify whether the actual use case(s) of the software tool match those evaluated by Synopsys
     - Verify whether the actual inputs and outputs are identical to or a sub-set of those as evaluated by Synopsys
     - Verify that all conditions of use (CoU) specified by Synopsys are met, or whether the development process can be adjusted to meet these CoU(s)
     - Verify that all assumptions of use (AoU) specified by Synopsys are met, or whether the development process can be adjusted to meet these AoU(s)
     - Verify that the pre-determined Tool Confidence Level (TCL) for the relevant use case(s) are TCL1, *or*
     - Verify that Synopsys has successfully performed an additional software tool qualification for all TCL2 and TCL3 scenarios to conclude that the tool is suitable to be used for the development of a safety-related element of the same or higher ASIL than required by the user
   - If all the verification steps described above are successful, then the results of the Synopsys software tool criterial evaluation (and qualification) are applicable to the tool user, which means:
     - The required TCL pre-determined by Synopsys can be taken over by the tool user for actual product development
     - If the pre-determined TCL is TCL1, then the tool can be used without the need to perform any additional software tool qualification
     - If the pre-determined TCL is TCL2 or TCL3, then the software tool qualification performed by Synopsys is sufficient, and the tool can be used without the need for further software tool qualification by the end user
   - All of the steps above must be documented in a software tool criteria evaluation report, including evidence for the successful conclusion of all verification steps, which may include reference to the Synopsys Functional Safety Manual, and optionally, to the Synopsys certification and assessment report

2. Software tool qualification
    - If any of the verification steps described above as part of the tool user's software tool criteria evaluation fails (e.g. different use case, CoU or AoU cannot be met, pre-determined TCL is not TCL1 and Synopsys has not performed a software tool qualification), then the user must perform his/her own software tool qualification
    - The specific methods applied for tool qualification are decided and planned by the tool user -- Synopsys does not recommend any specific methods or procedures
    - The summary of the qualification methods, procedures and results shall be documented in a software tool qualification report

4 Formality Description

This section provides a general description regarding the use of the Formality tool as a software tool in the development of safety-related applications and describes where to get the latest product documentation and the runtime environment required to use the Formality tool.

Coverage

The *Formality Functional Safety Manual* is intended to be used starting with the version 2017.09 and later versions of the Formality tool per the use cases presented in this document. In general, unless otherwise noted, the failure modes and detection mechanisms noted in the use cases presented in Section 6 are tool version independent.

Compliance with ISO 26262

The Formality tool can be used in the development of safety-related elements according to ISO 26262, with allocated safety requirements up to a maximum Automotive Safety Integrity Level D (ASIL D), if the tool is used in the context of a tool chain and in compliance with this document, the *Formality Functional Safety Manual*.

See the exida Certificate for ISO 26262 Compliance of Synopsys Formality when used in a tool chain flow.

Product Documentation and Support

Comprehensive documentation for using the Formality tool is provided on SolvNet. The latest documentation for the Formality tool can be accessed at Formality Online Help and the following usage guide documents on SolvNet:

- HDL Compiler for VHDL User Guide
- HDL Compiler for Verilog User Guide
- HDL Compiler for SystemVerilog User Guide

Specific documentation for performing design and analysis as part of an ISO 26262 compliant flow is provided in Section 3, Section 5, Section 6 and Appendix A of this document, the *Formality Functional Safety Manual*.

Synopsys provides online customer support for the Formality tool. See Section 1 for more information.

Installation and Supported Platforms

The installation of the Formality tool must follow the guidelines in the *Synopsys® Installation Guide* as well as the specific *Formality Installation Notes* document.

Users are required to download the tool executable and INSTALL_README from the SolvNet site at https://solvnet.synopsys.com/DownloadCenter/dc/product.jsp.

Supported platforms and operating systems requirements:

- For installation instructions, see the *Synopsys® Installation Guide* at https://www.synopsys.com/install.
- For the latest supported binary-compatible hardware platform or operating system, including required operating system patches, see https://www.synopsys.com/qsc.
- If updates (including security patches) to computing environments (including operating systems) are backward compatible with previous versions of the computing environment used to test the Formality tool, the results of the testing performed by Synopsys using such previous versions are applicable.

Additional information:

- For information about the compute platforms roadmap, go to https://www.synopsys.com/support/licensing-installation-computeplatforms/compute-platforms/compute-platforms-roadmap.html.
- For platform notices, go to https://www.synopsys.com/support/licensing-installation-computeplatforms/compute-platforms/platform-notice.html.
- For information regarding the license key retrieval process, go to https://solvnet.synopsys.com/smartkeys/smartkeys.cgi.

User Competence

To properly use the Formality tool, a user must have a good understanding and working knowledge of the following:

- Electrical engineering and circuit design
- The ISO 26262 standard
- Documentation of the Formality tool, such as the User Guide, at Formality Online Help on SolvNet
- This Functional Safety Manual
- The published list of safety-related defects for the Formality tool available at Formality Safety-Related Issues Master List
- Applicability of the Formality tool in the overall tool chain

Managing Known Safety-Related Defects

Synopsys maintains current information for every reported defect through STARs. The Formality team evaluates each reported issue for potential impact on functional safety.

A list of all known safety-related defects for each release of Formality is available on a SolvNet knowledge base article and is referenced from the *Formality Release Notes*.

Formality users must assess, as part of their own software tool criteria evaluation, the potential impact of the known safety-related defects in their design and must ensure mitigation of any relevant safety-related defects.

Managing New Releases

Synopsys can release new versions of the Formality tool at any time to extend its functionality or to fix defects. When a new version is available, notification is posted on the SolvNet site. A subscription service is available for users to be notified of any new product releases.

When installing a new version of the Formality tool, users must evaluate the impact of any known safety-related defects in their design by checking the accompanying *Formality Release Notes* for the following:

- Any changes that apply to safety-related use cases
- List of known safety-related defects in the new version of the Formality tool

In addition, users must refer to the latest version of this document, the *Formality Functional Safety Manual*, available with the product release contents.

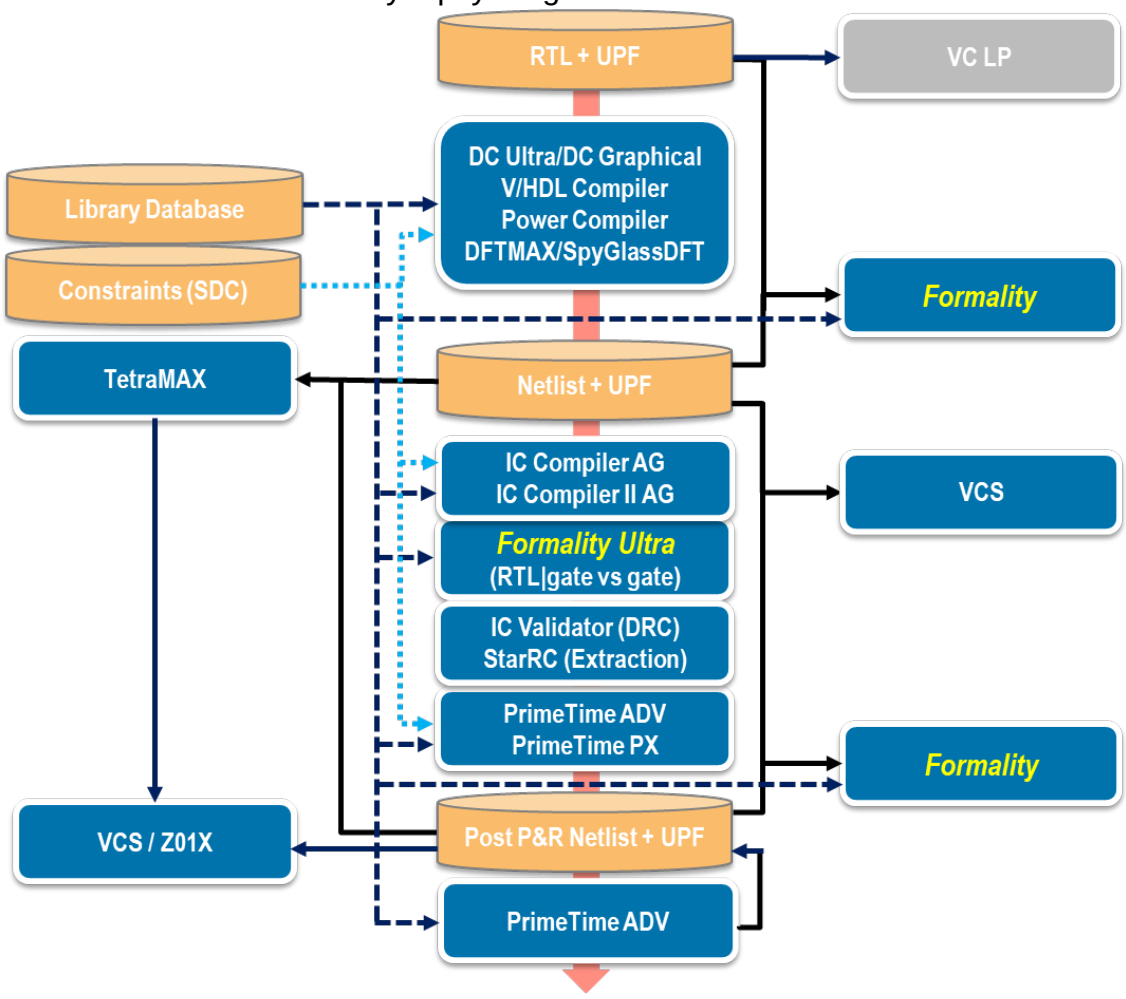
5 Synopsys Digital Tool Chain

This section provides an overview of where the Formality is used in the tool chain.

The ISO 26262 standard provides a methodology and requirements for software tool criteria evaluation and qualification (see ISO 26262-8, clause 11). It applies to software tools used for the development of safety-related designs where it is essential that the tool operates correctly without introducing or failing to detect errors in the safety-related design.

The suitability of a software tool to be used in the development of a safety-related design is determined in the software tool criteria evaluation, which results in a Tool Confidence Level (TCL): a level of confidence that the software tool does not introduce or fail to detect an error in the design without being noticed, and mitigated before the design is released as a safety-related product. This evaluation is best performed in the context of the overall software tool chain and development flow, in which the individual software tool is used. The following high-level diagram reflects the tool chain for which the Formality tool is applicable.

Synopsys Digital Tool Chain



6
Use Cases

This section describes the safety-qualified use cases of the Formality tool. Users should also perform TCL determination based on their specific Use Cases.

In the development from RTL to final Netlist, the design undergoes changes due to optimizations throughout the flow. We need a tool to ensure that the optimized design is still functionally equivalent to the original version of the design through each stage of optimization. The Formality tool is an equivalence checker. The purpose of the Formality tool is to detect unexpected differences that might have been introduced into a design during development. It uses a formal verification comparison engine to prove or disprove the equivalence of the two specified designs and presents any differences for further detailed analysis.

Formal verification is an alternative to verification through simulation. Formal verification uses mathematical techniques to compare the logic to be verified against a logical specification or a reference design. Unlike verification through simulation, formal verification does not require input vectors. As formal verification considers only logical functions during comparisons, so it is independent of a design's physical properties, such as layout and timing.

Use Case 1: Equivalence Check

In this use case, the goal is to compare a tool-modified netlist with the original version of the design for identifying unexpected differences during the design development. It compares RTL-to-Gate and Gate-to-Gate netlists.

Figure 3 shows the basic flow to verify a single-design process. The Formality tool reads the files, the reference Design A and the implementation Design B. After reading the files, the tool establishes the points in the design that are candidates to be compared, matches them between the two designs as appropriate, performs the formal equivalence check, and reports any differences that are detected.

- Affected tool: Formality

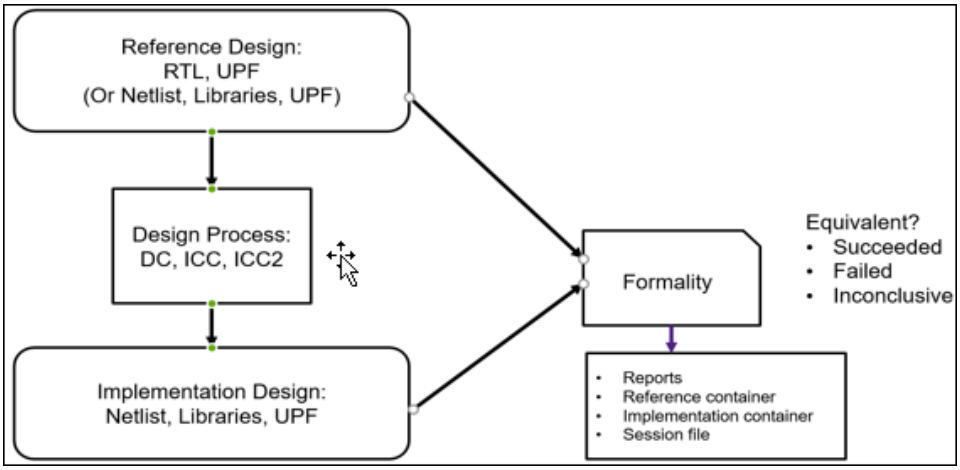


Figure 3: Verification Flow Using Formality

In this use case, the Formality tool uses and generates the following main inputs and outputs.

- Inputs:
  - Reference Design (RTL or Netlist and UPF if used)
  - Implementation Design (Netlist and SVF, and UPF if used)
  - Verilog simulation libraries or .db libraries
  - Formality Tcl Scripts
- Expected outputs:
  - Transcript log (outputs to support debugging sessions that are not considered as the debugging process is not safety relevant. Only final passing verification is considered safety relevant.)

For this use case of the Formality tool, the following conditions of use (constraints for the design and design environment, recommended procedures for the tool usage, etc.) shall be met:

- CoU-FM-001: User shall not continue with an error and shall review all warnings to take appropriate action.
- CoU-FM-002: User shall follow the Formality Reference Methodology scripts.
- CoU-FM-003: For the final run, the Tcl script-based batch mode execution shall be used, without using the interactive command line or the GUI manual command entry. Tcl scripts and log files shall be retained as design signoff records.
- CoU-FM-004: The Formality tool does not verify scan chain and BIST logic that exist in the netlist because it does not exist in RTL. Therefore, scan chain needs to be disabled before verifying.

For this use case of the Formality tool, the following assumptions of use (required actions to be taken by the tool user to prevent or detect design errors due to possible tool malfunctions) shall be met:

- AoU-FM-001: User shall review the transcript log for error and warning messages, completeness (no missing sections), and integrity (no corruption).
- AoU-FM-002: User shall check that the transcript log is generated with an up-to-date timestamp.
- AoU-FM-003: User shall ensure that the transcript log has the "Verification SUCCEEDED" statement.
- AoU-FM-005: User shall ensure that only the synthesizable subset of HDL will be used as RTL input.

All analyzed failure modes and prevention, detection and mitigation measures (including conditions and assumptions of use listed above) are independent of the exact Formality tool version.

A software tool criteria evaluation performed by Synopsys according to ISO 26262-8, clause 11, which assumes the fulfillment of all conditions of use (CoU) and assumptions of use (AoU) as described above, results in a required tool confidence level:

TCL1 for *Formality* Use Case 1: Equivalence Check

In this case, no further activities for software tool qualification are required.

Use Case 2: Formality Ultra Verification

In this use case, the goal is to interactively modify the original netlist and verify it against ECO RTL. It compares the ECO RTL netlist with the original netlist, see Use Case 1.

- Affected tools:
  - Formality
  - Formality Ultra

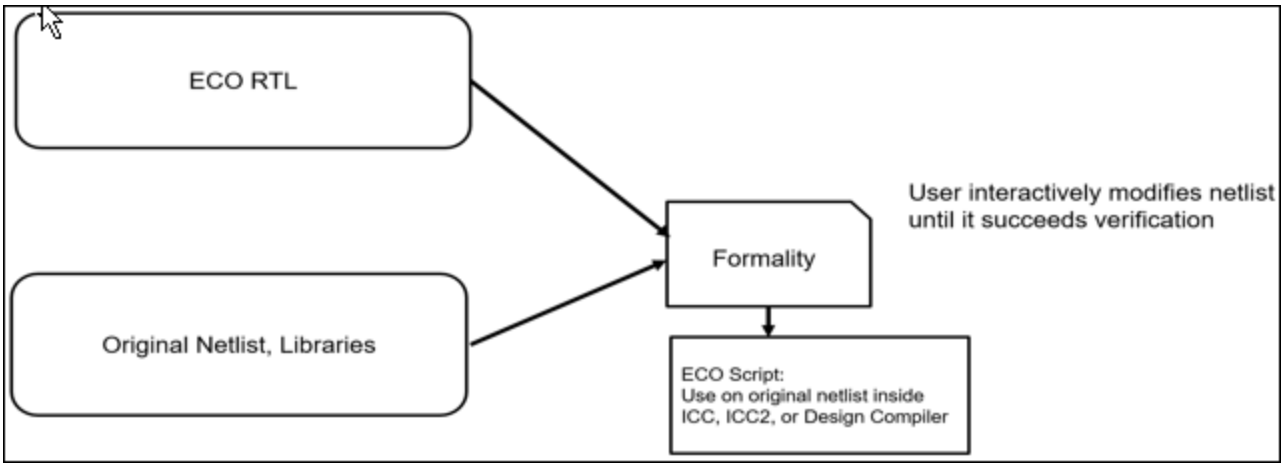


Figure 4: Formality Ultra and ECO Script generation

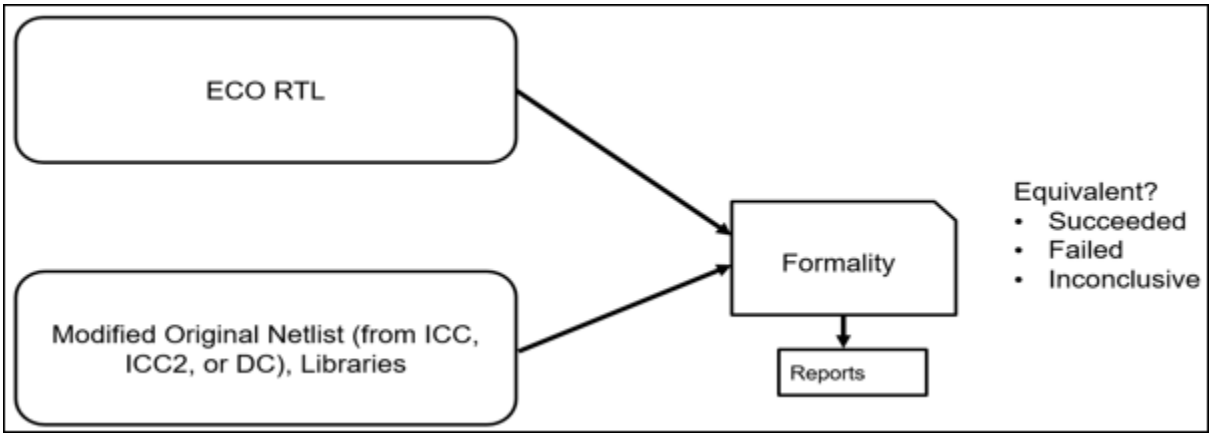


Figure 5: Formality Ultra and Verifying Modified Netlist With ECO RTL

In this use case, the Formality tool uses and generates the following main inputs and outputs.

- Inputs:
  - Reference Design (ECO RTL and UPF if used)
  - Implementation Design (original netlist and original SVF and SVF' resulting from RTL line number changes; and UPF if used)
  - Verilog simulation libraries or .db libraries
  - Formality Tcl Scripts
- Expected outputs:
  - Transcript log (outputs to support debugging sessions that are not considered because the debugging process is not safety relevant. Only final passing verification is considered safety relevant.)
  - ECO patch script (using Tcl script for the Design Compiler, IC Compiler, or IC Compiler II tool with low-level edit commands for modifying the original netlist to make it

functionally equivalent with ECO RTL. This flow expects to use equivalence checking for verifying the final, modified netlist from the Design Compiler, IC Compiler, or IC Compiler II tool against the ECO RTL.)

For this use case of the Formality tool, the following conditions of use (constraints for the design and design environment, recommended procedures for the tool usage, etc.) shall be met:

- CoU-FM-001: User shall not continue with an error and shall review all warnings to take appropriate action.
- CoU-FM-002: User shall follow the Formality Reference Methodology scripts.
- CoU-FM-003: For the final run, the Tcl script-based batch mode execution shall be used, without using the interactive command line or the GUI manual command entry. Tcl scripts and log files shall be retained as design signoff records.
- CoU-FM-004: The Formality tool does not verify scan chain and BIST logic that exist in the netlist because it does not exist in RTL. Therefore, scan chain needs to be disabled before verifying.

For this use case of the Formality tool, the following assumptions of use (required actions to be taken by the tool user to prevent or detect design errors due to possible tool malfunctions) shall be met:

- AoU-FM-001: User shall review the transcript log for error and warning messages, completeness (no missing sections), and integrity (no corruption).
- AoU-FM-002: User shall check that the transcript log is generated with an up-to-date timestamp.
- AoU-FM-003: User shall ensure that the transcript log has the "Verification SUCCEEDED" statement.
- AoU-FM-004: User shall run equivalence checking on modified netlist inside the Formality tool before generating the ECO Tcl script.
- AoU-FM-005: User shall ensure that only the synthesizable subset of HDL will be used as RTL input.

All analyzed failure modes and prevention, detection and mitigation measures (including conditions and assumptions of use listed above) are independent of the exact Formality tool version.

A software tool criteria evaluation performed by Synopsys according to ISO 26262-8, clause 11, which assumes the fulfillment of all conditions of use (CoU) and assumptions of use (AoU) as described above, results in a required tool confidence level:

TCL1 for *Formality* Use Case 2: Formality Ultra Verification

In this case, no further activities for software tool qualification are required.

Use Case 3: Formality Library Verification

In this use case, the goal is to compare all the cells in a reference library with all the cells in an implementation library. These include Verilog, simulation, and Synopsys (.db) synthesis libraries.

- Affected tools: Formality

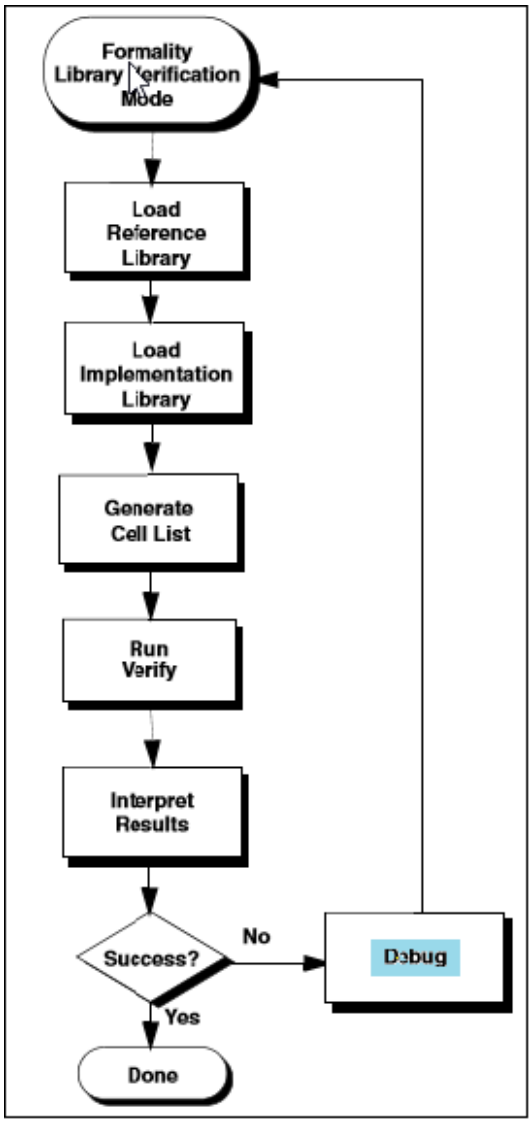


Figure 6: Formality Library Verification Flow

In this use case, the Formality tool uses and generates the following main inputs and outputs.

- Inputs:
  - Synopsys .db libraries
  - Verilog Libraries
  - Verilog User Defined Primitives Libraries
  - Synopsys power .db libraries
- Expected outputs:
  - Transcript log (outputs to support debugging sessions that are not considered because the debugging process is not safety relevant. Only final passing verification is considered safety relevant.)

For this use case of the Formality tool, the following conditions of use (constraints for the design and design environment, recommended procedures for the tool usage, etc.) shall be met:

- CoU-FM-001: User shall not continue with an error and shall review all warnings to take appropriate action.
- CoU-FM-002: User shall follow the Formality Reference Methodology scripts.
- CoU-FM-003: For the final run, the Tcl script-based batch mode execution shall be used, without using the interactive command line or the GUI manual command entry. Tcl scripts and log files shall be retained as design signoff records.

For this use case of the Formality tool, the following assumptions of use (required actions to be taken by the tool user to prevent or detect design errors due to possible tool malfunctions) shall be met:

- AoU-FM-001: User shall review the transcript log for error and warning messages, completeness (no missing sections), and integrity (no corruption).
- AoU-FM-002: User shall check that the transcript log is generated with an up-to-date timestamp.
- AoU-FM-003: User shall ensure that the transcript log has the "Verification SUCCEEDED" statement.
- AoU-FM-005: User shall ensure that only the synthesizable subset of HDL will be used as RTL input.

All analyzed failure modes and prevention, detection and mitigation measures (including conditions and assumptions of use listed above) are independent of the exact Formality tool version.

A software tool criteria evaluation performed by Synopsys according to ISO 26262-8, clause 11, which assumes the fulfillment of all conditions of use (CoU) and assumptions of use (AoU) as described above, results in a required tool confidence level:

TCL1 for *Formality* Use Case 3: Formality Library Verification

In this case, no further activities for software tool qualification are required.

7
Limitations of Use Cases

This section describes all known limitations of the use cases mentioned in the previous section.

All known safety-related issues for the Formality tool are listed in the Formality Safety-Related Issues Master List available on SolvNet.

LIM-1: Inconclusive Verification result

Formal verification can result in an inconclusive verification. This is a technology limitation and can occur when the Formality tool is unable to determine whether the reported compare points are equivalent.

LIM-2: RTL-to-Design Compiler Gate (with SCAN) verification

The Formality tool does not verify scan chain and BIST logic that exists in the netlist because it does not exist in RTL. Therefore, scan chain needs to be disabled before verifying.

LIM-3: Legacy clock-gating in Formality

The legacy clock-gating method used by the Formality tool has a few limitations when identifying the clock-gating logic resulting during optimization. The user can enable the verification_clock_gate_edge_analysis variable as an alternative during these instances.

LIM-4: Library verification mode

In the library verification mode, the Formality tool supports only the verification of Verilog and .db formats.

Appendix A
Software Tool Information

This section provides general information about the Formality software tool, which is needed by the tool user for performing his/her software tool criteria evaluation.

The following information about Formality is required according to ISO 26262-8, for the planning of the usage of a software tool (clause 11.4.4) and the preparation of the own software tool criteria evaluation (clause 11.4.5).

Please note that some of the information below provided by Synopsys simply needs to be confirmed by the tool user and can be used without modification. Other information must be completed or updated by the tool user to reflect his/her actual situation.

Required Info	**Tool Information**	**Reference / Comment**
Tool vendor	Synopsys, Inc.	ISO 26262-8, 11.4.4.1.a
Tool name and version	Formality Formality Ultra	ISO 26262-8, 11.4.4.1.a To determine tool version, use: `report_version -options`
Tool use cases		ISO 26262-8, 11.4.4.1.c ISO 26262-8, 11.4.5.1.a To be completed by the tool user. Align with / verify against use cases described in Section 6 of this document.
Tool inputs and expected outputs		ISO 26262-8, 11.4.5.1.b To be completed by the tool user. Align with / verify against inputs and outputs described in Section 6 of this document.
Tool configuration and constraints		ISO 26262-8, 11.4.4.1.b ISO 26262-8, 11.4.5.1.c To be completed by the tool user. Align with / verify against CoU for the use cases described in Section 6 of this document.

Required Info	Tool Information	Reference / Comment
Tool environment (OS)	Refer to Formality Installation Notes at https://solvnet.synopsys.com/DownloadCenter. Click on Formality, then the release number, such as 2017.09, and then "View installation guide" for version-specific OS support.	ISO 26262-8, 11.4.4.1.d To be completed by the tool user. Align with / verify against the OS version evaluated by Synopsys. To determine Linux version, use: `uname -osr`
Tool environment (CAD tool chain)		ISO 26262-8, 11.4.4.1.d To be completed by the tool user. To determine name and version of your tool chain, please consult your CAD department.
Maximum ASIL	ASIL D	ISO 26262-8, 11.4.4.1.e
Tool qualification methods	Not applicable	ISO 26262-8, 11.4.4.1.f Software tool qualification is not required for Formality
User manual and other usage guide documents	See Product Documentation and Support in Section 4 of this document.	ISO 26262-8, 11.4.4.2.a – d Tool user to include a link to these documents (Synopsys SolvNet or local copy), and to add any additional company-internal tool usage guidelines.
Known software tool malfunctions, and appropriate work arounds ...	For limitations, refer to Section 7 of this document. For the list of Safety-Related Issues Master List, see User Competence in Section 4 of this document.	ISO 26262-8, 11.4.4.2.e Tool user to include a link to these documents (Synopsys SolvNet or local copy), and to add any additional company-internal work around descriptions.
Measures for the detection of tool malfunctions ...		ISO 26262-8, 11.4.4.2.f To be completed by the tool user. Align with / verify against AoU for the use cases described in Section 6 of this document.

Required Info	Tool Information	Reference / Comment
Measures for the detection of tool malfunctions ...		ISO 26262-8, 11.4.4.2.f To be completed by the tool user. Align with / verify against AoU for the use cases described in Section 6 of this document.

Appendix B
Complete List of CoU and AoU IDs

The complete list of Conditions of Use (CoU) for Formality is in the table below. CoU defines a condition of the design, software tool, design environment, or situation that is assumed and required to be fulfilled by the user.

ID	Description
CoU-FM-001	User shall not continue with an error and review all warnings to take appropriate action.
CoU-FM-002	User shall follow the Formality Reference Methodology scripts.
CoU-FM-003	For the final run, Tcl script-based batch mode execution shall be used, without interactive command line entry or GUI manual command entry. Tcl scripts and log files shall be retained as design signoff records.
CoU-FM-004	The Formality tool does not verify scan chain and BIST logic that exist in the netlist because it does not exist in RTL. Therefore, scan chain needs to be disabled before verifying.

The complete list of Assumptions of Use (AoU) for Formality is in the table below. AoU defines an action that is assumed and required to be taken by the user of a software tool.

ID	Description
AoU-FM-001	User shall review the transcript log for error and warning messages, completeness (no missing sections), and integrity (no corruption).
AoU-FM-002	User shall check that the transcript log is generated with an up-to-date timestamp.
AoU-FM-003	User shall ensure that transcript log has "Verification SUCCEEDED" statement.
AoU-FM-004	User shall run equivalence checking on modified netlist inside the Formality tool before producing ECO Tcl script.
AoU-FM-005	User shall ensure that only the synthesizable subset of HDL will be used as RTL input.