SIEMENS
Ingenuity for life

Siemens Digital Industries Software

Automating clock-domain crossing verification for DO-254 (and other safety-critical) designs

Executive summary

Metastability is a serious problem in safety-critical designs, frequently causing chips to exhibit intermittent bugs that may not be caught until an in-flight failure. Traditional simulation does not accurately analyze multi-clock designs and relies on a manual, error-prone process. This paper describes the automated clock domain crossing verification solution DO-254 projects need and tool assessment tips.

Kurt Takara
Siemens EDA

Contents

Overview of DO-254

The focus of Document RTCA/DO-254 "Design Assurance Guidance for Airborne Electronic Hardware" (referred to herein as "DO-254") is hardware reliability for flight safety. In other words, the FAA, EASA and other aviation authorities intend to ensure that the complex electronic hardware used in avionics works reliably as specified, avoiding faulty operation and potential air disasters. DO-254 defines a process that hardware vendors must follow to get their hardware certified for use in avionics. DO-254, which the FAA began enforcing in 2005 (through AC20-152), is modeled after DO-178B, the equivalent process for certifying software, which was published in its original version (DO-178) over 25 years ago. All in-flight hardware (i.e. FPGA or ASIC designs) must now comply with DO-254.

NOTE: This document does not provide general information on the DO-254 process, but rather focuses on the issue of clock-domain crossing verification and tool assessment, specifically for the tool Questa CDC. If you need general information or training on the DO-254 process, we advise that you visit the DO-254 user's group web site (www.do-254.com).

The problem with clock-domain crossing (CDC)

Metastability is the term used to describe what happens in digital circuits when the clock and data inputs of a flip-flop change values at approximately the same time. This is not a problem in single-clock designs, but this becomes a problem on paths transmitting data between asynchronous clock domains. When the data changes in the setup/hold window, this leads to the flip-flop output oscillating and settling to a random value, as shown in figure 1. In this case, the output of the flip-flop is said to have gone metastable and will lead to incorrect design functionality, such as data loss or data corruption on CDC paths. This situation happens in every design containing multiple asynchronous clocks, which occurs any time two or more discrete systems communicate.

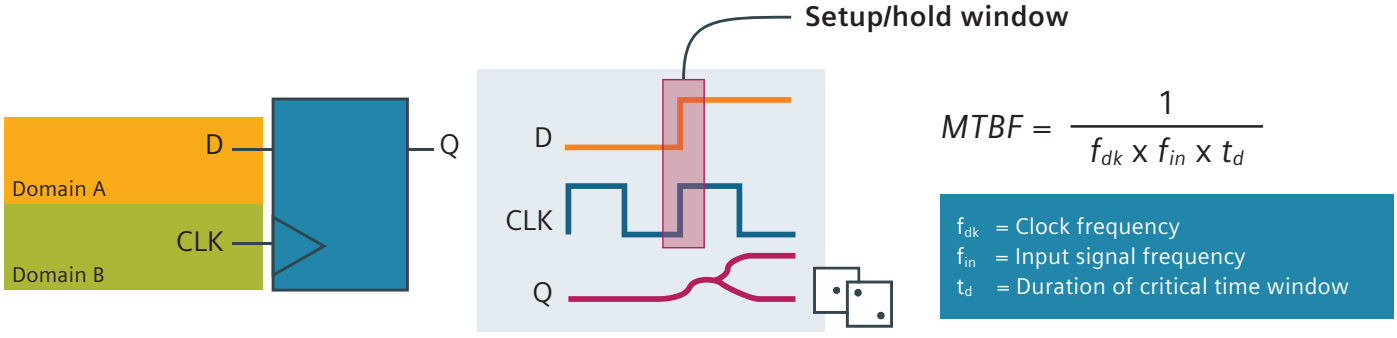

Figure 1: Clock domains, metastability and mean time between failure calculations.

Metastability is a serious problem in safety-critical designs in that it frequently causes chips to exhibit intermittent failures. These failures generally go undetected during simulation (which tests a chip's logic functions) and static timing (which tests for timing – within a single clock domain). A typical verification methodology simply does not consider potential bugs from clock-domain crossing paths. Thus, if CDC paths are not explicitly verified, CDC bugs are typically identified in the actual hardware device in the field. For DO-254 projects, catching faulty operation "in the field" means *critical bugs may not be caught until an in-flight failure.*

With today's highly integrated and concurrent designs, the number of independent clock domains found on the typical device is growing. According to an industry research study performed by Wilson Research in 2018, the average number of clock domains on a single device was between 5-10. This means that the probability of metastability bugs has grown substantially from previous designs.

The real issue is that traditional simulation and timing analysis do not accurately analyze multi-clock designs. Designers are generally aware of the metastability problem and try to implement logic to isolate the outputs of the metastable registers such that this metastable value does not propagate into the rest of the design. For example, experienced designers add synchronizers between clock domains, create protocols for transferring data between domains, and try to avoid situations where data from multiple clock domains reconverge, as shown in figure 2.

However, it is quite easy to leave out needed synchronizers, or place one incorrectly such that it does not work as expected. Even careful manual code reviews easily miss these problems. Reconvergence issues, one of the most dangerous and insidious CDC problems, are almost impossible to find through manual code reviews. The effects of CDC issues can be highly data dependent, and may only exhibit themselves in corner case situations when a combination of a specific data value crosses the CDC boundary while the design is in a specific vulnerable state.

To make matters worse, verification engineers – who generally are not as well versed in design as the designers themselves – often do not recognize these types of CDC issues. This is one situation when the independence of design and verification roles, as required by DO-254, could be potentially harmful.

Finally, after completing RTL verification, changes that are introduced in the design during the implementation process, such as logic optimization, physical optimization and introduction of design-for-test (DFT) logic and low-power logic, may cause incorrect behavior on CDC paths as well as introduce new CDC paths. For example, incorrect combinational logic generated by synthesis tools

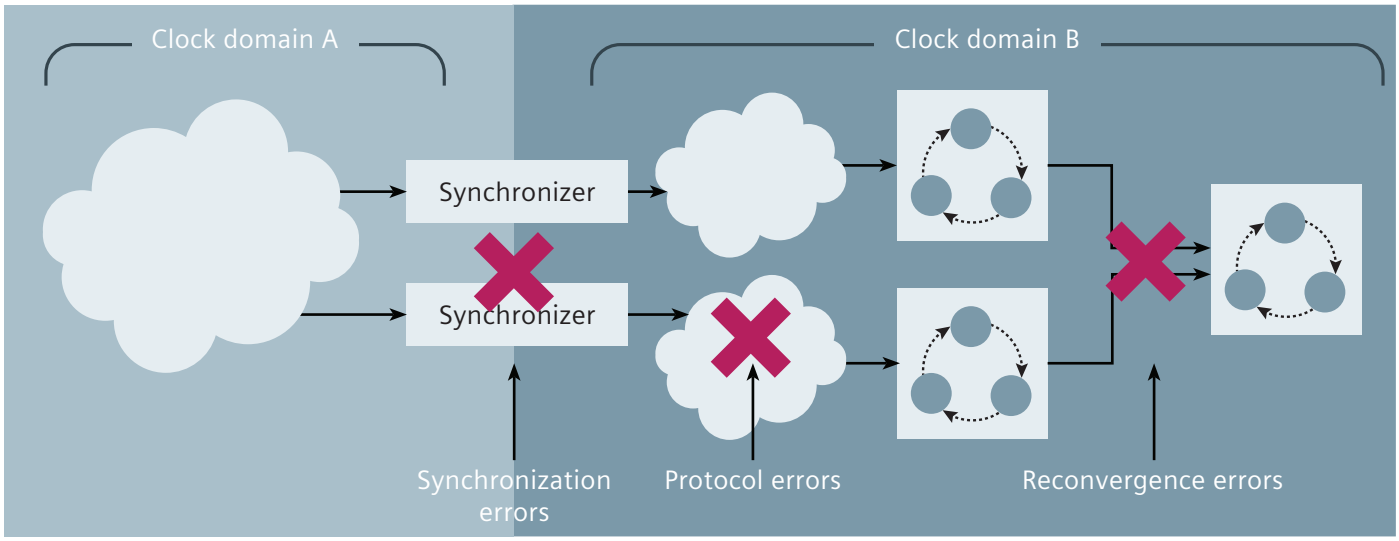

Figure 2: Potential CDC errors.

may result in glitches on CDC paths (Figure 3). *Refer to Appendix A for more information on how designers try to address CDC issues and what can go wrong.*

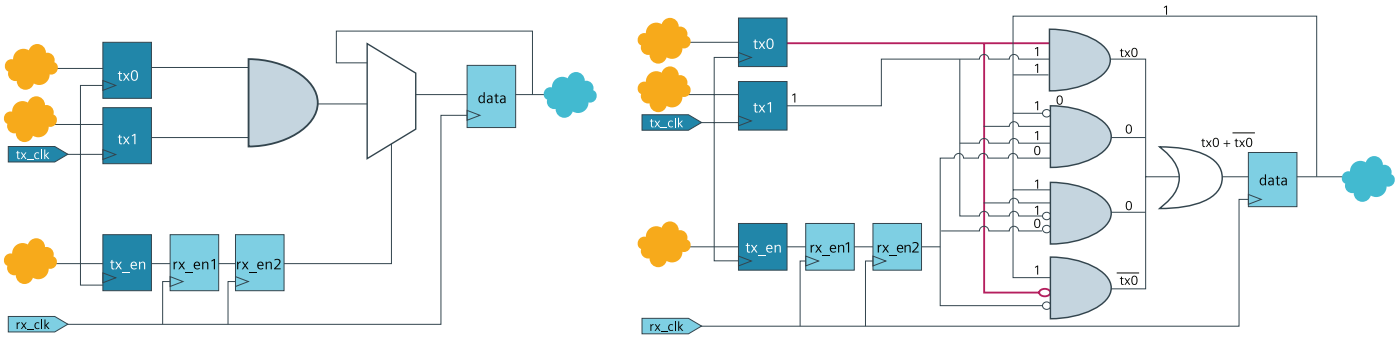

Figure 3: Synthesis introduces glitches on CDC paths.

Applying CDC on DO-254 designs

Airborne systems go through several safety assessment processes. As a result, the DO-254 project is assigned a design assurance level (DAL) of A through E. The level corresponds to the criticality of a resulting failure. For example, a failure in a level A design would result in catastrophic conditions (such as the plane crashing), while a failure in a level E design might simply mean that some passengers could be subject to minor inconvenience. Level A (Catastrophic) and level B (Hazardous/Severe/Major) projects must not only follow DO-254 processes but must also address additional safety concerns. (Refer to the DO-254 specification for complete details on DO-254 and additional requirements for level A/B designs).

For the sake of safety (or rather design assurance), CDC verification should be employed on every level A/B airborne design with multiple asynchronous clock domains. While DO-254 does not explicitly mandate the verification of clock-domain crossings, understanding the history and purpose of the DO-254 document sheds light on the reason.

First, the beginnings of the DO-254 spec were drafted nearly twenty years ago. At that time, while the issue of clock-domain crossing and metastability were known, it was not very common to have devices with multiple asynchronous clock domains. However, in the last ten years, highly integrated devices have become the norm in many segments of the electronics industry. Today these same trends have found their way into military/aerospace designs as well. So at the time of the DO-254 writing, CDC was not a very prominent issue and there were no tools to deal with it. The best that could be done was that designers had to be cognizant of CDC issues and be careful in their design practices.

Second, DO-254 is designed to be flexible, and thus, generally does not mandate the use of any particular technique. DO-254 is designed to be open and evolve with the electronic devices themselves and their corresponding design/verification techniques. Thus, DO-254 mandates that objectives be met, but rarely specifies "how" to meet these objectives. This is important in that DO-254 requirements do not become obsolete as new and better methods evolve.

DO-254 does advocate for thorough verification in the name of safety. As part of its general guidance, it lists "some methods that may be applicable to both validation and verification" (section 6.3). One such method is "Design Margin Analysis" which is defined as *"verifies that the design implementation satisfies its functional requirements given the variability of components."* CDC fits within this category of analysis, as the variability of clock timing between independent domains can impact device function and should therefore be analyzed. In addition, design implementation may introduce CDC bugs when synchronization structures are incorrectly synthesized.

Additional design assurance strategies may be required for hardware designs, or paths within those designs, that are found to be safety-critical. As part of the DO-254 process, a hardware safety assessment is done in conjunction with a system safety assessment (section 2.3). This assessment determines the hardware design assurance level, which in turn dictates the types of design assurance strategies required. Designs are designated as having design assurance levels A-E, with levels A and B having "catastrophic" and "major" impact on aircraft function in case of failure.

For devices categorized as level A/B, a set of requirements will be derived to address the safety requirements. The DO-254 guidance specifically states (section 2.3.4): *"For Level A or B functions implemented in hardware, the design assurance considerations should address potential anomalous behaviors and potential design errors of the hardware functions."*

Appendix A section 3.3 also discusses advanced verification methods, one of which is safety-specific analysis, whose aim is to check for not only *"intended-function requirements verification, but also for anomalous behaviors."* Susceptibility to metastability can be defined as an anomalous behavior resulting from incorrect hardware design.

To summarize, in order to understand CDC in the context of DO-254, consider the purpose of DO-254 – design assurance. A DO-254 methodology should ensure that a device is going to behave as specified, and that everything possible is done to catch bugs before the device will be operating in flight. Thus, the issue of verifying CDCs should be a requirement by design projects. In fact, some primary contractors recognize this issue and in some cases are adopting CDC as part of their own verification methodologies and/or are placing requirements on their sub-contractors to test for CDC issues.

Automating CDC verification

Even if the verification team does recognize the problems associated with CDCs, verifying metastability effects and CDC by hand is very difficult and extremely error prone. Therefore, companies should use an automated solution designed specifically for CDC verification to bridge the knowledge gap between design and verification teams, and to ensure comprehensive coverage of this problem.

However, not all automated solutions are equivalent. Some tools only do a partial job of finding CDC bugs. A comprehensive CDC verification solution, such as that offered by Questa CDC, must do four distinct things:

1. Perform a structural analysis. This is most effectively done on the RTL code to identify and analyze all signals crossing clock domains, and determine if their synchronization schemes are present and correct.
2. Verify transfer protocols. This assures that the synchronization schemes are used correctly, by monitoring and verifying that protocols are being followed during simulation or formal analysis.
3. Globally check for reconvergence. This is most effectively done by injecting the silicon-accurate effects of potential metastability into the RTL simulation environment and verifying that the design will function correctly.

4. Netlist glitch analysis. This structural analysis on the design netlist identifies glitchy logic introduced by synthesis.

The combination of these four aspects of CDC verification is very powerful. Hands down it is far superior to any sort of manual method. While an extensive manual code review could find structural issues (e.g., are all the synchronizers in place), it would be tedious, time consuming and error prone. In addition, manual reviews typically cannot ensure that transfer protocols are always used correctly, and almost never address reconvergence issues. Finally, RTL verification is not sufficient, since implementation may introduce CDC issues after RTL verification completion.

Consumer electronics and storage

Many companies have recognized this and have adopted Questa CDC as an added design assurance strategy within their verification arsenal. Consider the following real-world cases.

U.S.-based storage/networking company
A new team in the company reused a block of code that had been modified by many people. They understood CDC issues and were taking precautions to ensure metastability did not affect the operations of their components. But to be sure, they ran Questa CDC on the device. The tool found 60+ errors, some of which could have been critical and costly had they gone undetected until the end systems shipped to customers. This caused management to require CDC checking on the other blocks in the design. A clean Questa CDC run is now a requirement before a block or design can be released. Word is spreading throughout the company as more and more groups are now using this technique as part of their verification methodologies for added assurance and to minimize risk of late-stage, costly bugs in hardware.

Large global computer company
This group was designing a Dual port Ethernet Controller with 12 clock domains, and most of the logic was reused and thought to be good. The new use of the reused design changed the clocking scheme, which created a synchronization issue in a correctly designed block. They told us "Questa CDC indeed found a synchronization bug in a reused design that was supposed to be good!" This saved the company a very expensive respin.

Large Japanese consumer products company
This company, which makes a wide range of consumer products, has become an avid user of Questa CDC after having previously struggled with undetected CDC problems. They tell us: "We found several CDC bugs with Questa CDC. We have now trained more than 300 designers on Questa CDC and use Questa CDC all our products."

U.S.-based wireless communications provider
This company has been performing CDC verification for years and is currently using CDC verification tools across their company at many sites on many projects. They realize the value of a thorough CDC verification solution. One of the key proponents of CDC solutions within this company did a competitive analysis of Questa CDC versus another popular tool and his findings were published here: http://www.deepchip.com/items/0468-08.html.

Storage devices, computers, consumer products and wireless communications – it's unlikely that any of these systems will risk lives if they fail. Yet these companies are all seeing tremendous value in automating the verification of clock-domain crossings.

Mil-Aero

Companies in the military/aerospace market are also beginning to see the problems associated with CDCs and the value of an automated verification solution. In these applications, failures can be catastrophic, making exhaustive, accurate CDC verification even more critical.

A maker of military space systems
A company that designs missiles, satellite systems and other applications discovered the value of Questa CDC. This company had suffered from CDC bugs in the past. On one of their designs, a key engineer had been concerned that reconvergence of synchronized signals could be a problem, but had no way of knowing. He tried out the Questa CDC tool and found a real bug involving multiple independently synchronized signals that fed the next-state logic. Management realized that had such a problem gone undetected, it could jeopardize the

safe operations of their systems. The company decided to use Questa CDC on this project.

Large aerospace technology company
This company, who is starting to employ DO-254 level A/B methodology on many of its designs, has acknowledged that CDC bugs can be critical. On a recent design, a late-breaking design change introduced a CDC bug that took weeks to debug in the lab. They now beginning deploy Questa CDC as part of their standard design flow company-wide to catch these issues early on in their design flow.

Defense and aerospace systems supplier
A well-respected defense and aerospace systems supplier recognized the growing complexity and potential severity of CDC problems. In response to these concerns, they conducted an in-house study utilizing the Questa CDC tool, and found concrete evidence that CDC errors can slip through traditional design reviews. This study drove a change to the corporate wide design process to add a requirement for automated CDC analysis for every design. The company fully recognizes that catching these type of potential errors early in the design cycle will reduce lab integration time and improve system reliability. According to the engineer who drove this study, "The Questa CDC tool does a fantastic job of identifying CDC violations, and will help us eliminate this potential problem long before we enter the lab. This has long been a difficult design problem, but now we finally have tools that can formally prove that our designs are complete and free from the question of hidden CDC issues."

Questa CDC has been available for years and has been proven on thousands of industry designs. Thus, the problem of undetected metastability bugs is solved, but only if it is understood and addressed during verification. Every multi-clock, safety-critical design, especially those subject to DO-254 compliance, should specifically run CDC checking as part of a thorough verification process.

Tools assessment and DO-254

One key aspect of the DO-254 process is to determine that the tools used to create and verify designs are working properly. The process to ensure this is called "tool assessment" (though it is often mistakenly called "tool qualification"). Tool qualification is one method of tool assessment.

The purpose of tool assessment (and potentially tool qualification) is to ensure that tools that automate, minimize, or replace manual processes for hardware design and/or verification perform to an acceptable level of confidence on the target project. Tools are classified as either design tools or verification tools, depending on which design flow processes they automate. Likewise, as mentioned previously, designs are designated with a criticality level (A-E) that corresponds to the resulting severity of failure. The rigor of the tool assessment process depends on both the tool classification as well as the criticality level of the designated project.

Section 11, "Additional Considerations" of the DO-254 specification discusses "Tool Assessment." Figure 4 shows the flow diagram presented in this section of the specification.

The tool assessment and qualification process takes one of three forms:

Independent output assessment (see item 3 in figure 4): This means that another independent tool or method must validate the results of the tool.

Relevant history (see item 5 in figure 4): This means the tool has been previously used and has been shown to provide acceptable results.

Tool qualification (see item 7 in figure 4): This requires establishing and executing a plan to confirm that the tool produces correct outputs for its intended application.

Regardless of these classifications, the task of tool assessment falls upon the airborne applicant or airborne integrator (not the tool vendor). The applicant or integrator proposes the method of tool assessment as part of the DO-254 planning and documentation. The certification agency or its representative (in North America, this would be a Designated Engineering Representative, or DER) will determine if the proposed method of compliance to this requirement is adequate for the development process.

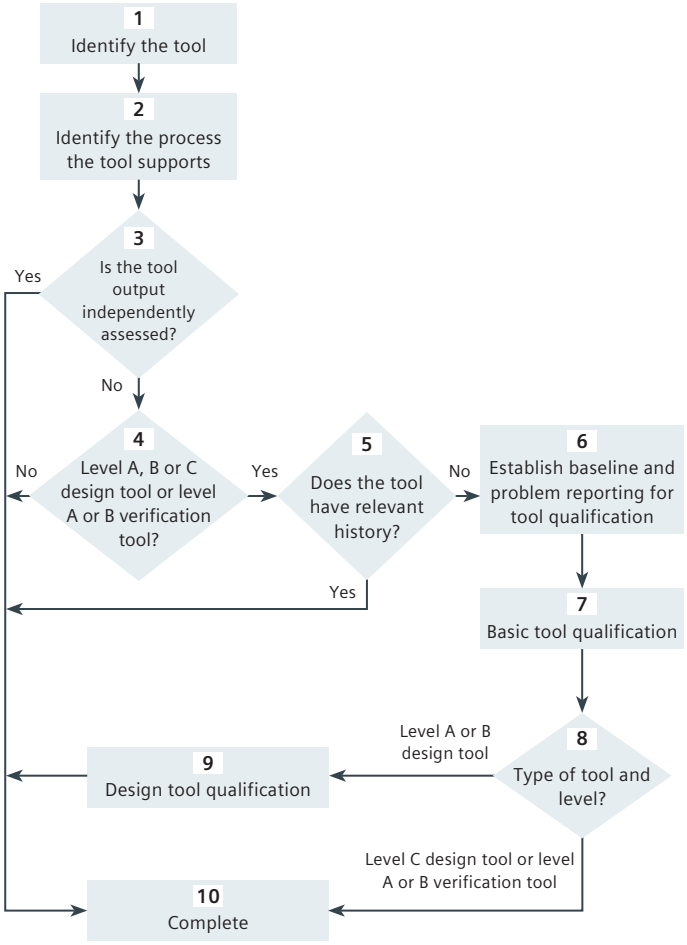

Figure 4: Design and verification tool assessment and qualification flow.

Key methods for tool assessment and qualification

The following are the DO-254 descriptions of the key methods for tool assessment and qualification. Clarification on how these apply to Questa CDC is covered in the next section.

Independent output assessment

An independent assessment verifies the correctness of the tool output using an independent means. If the tool output is independently assessed, then no further assessment is necessary. Independent assessment of a verification tool's output may include a manual review of the tool outputs or may include a comparison against the outputs of a separate tool capable of

performing the same verification activity as the tool being assessed. The applicant may propose other methods of independent assessment as well.

Relevant history
When it is possible to show that the tool has been previously used and has been found to produce acceptable results, then no further assessment is necessary. A discussion of the relevance of the previous tool usage versus the proposed usage of the tool should be included in the justification. Note: The history of the tool may be based on either an airborne or non-airborne application, provided that data is available to substantiate the relevance and credibility of the tool's history.

Basic tool qualification
...if no such relevant history can be evidenced, then the tool must under go "basic tool qualification" which includes tool configuration control, a tool problem reporting process, and a process to confirm that the tool produces correct outputs for its intended application using analysis or testing.

Qualifying Questa CDC for DO-254 designs

While a tool vendor cannot assess or qualify their own tools and the FAA does not provide blanket approval for use of any tools in DO-254 projects, what follows are explanations and suggestions for getting through the assessment process for Questa CDC, as easily as possible.

The first thing to ask when considering using Questa CDC on a DO-254 project is "Do I even need to mention it?" In other words, not all tools have to be identified and described in the "Plan for Hardware Aspects of Certification" (PHAC) or other DO-254 documents. You only have to do this if you want to claim credit for their use, and you only need to claim credit for use of a tool if there is some project requirement that must be fulfilled by using this tool.

Questa CDC provides added assurance that the design will function correctly within the intended system (remember, this is the intent of DO-254). However, unless you have a specific requirement identified by your end customer that says you must verify your clock domain crossings, you can just run Questa CDC on your project without it becoming part of the DO-254 review process. On the other hand, if you have a specific requirement from your customer (or even your DER) that says you must verify your clock domain crossings to identify and eliminate metastability issues, then you will have to choose a method of tool assessment. The simplest one by far is Independent Output Assessment. In this case, you would specify something similar to the following:

> *The results of the tool Questa CDC are checked independently by thorough testing in the lab. Lab testing will run extensive tests of the real hardware under real system clocking frequencies and should check all the conditions that were analyzed with Questa CDC.*

Conclusion

DO-254 methodologies must ensure that a device is going to behave as specified, and that everything possible is done to catch bugs before the device will be operating in flight. Thus, the issue of verifying CDCs should be a requirement by design projects. Since verifying metastability effects and CDC by hand is very difficult and extremely error prone, DO-254 projects should use an automated solution such as Questa CDC designed specifically for CDC verification to bridge the knowledge gap between design and verification teams, and to ensure comprehensive prevention of this problem.

Two appendices are included on the following pages.

1. Appendix A: manual CDC design methods and what goes wrong
2. Appendix B: glossary

Appendix A: Manual CDC design methods and what goes wrong

Most companies have requirements associated with designs containing multiple clock domains.

These include:

- Designers must use specific clock synchronization schemes, such as the 2D flip-flop synchronizer, or they must choose from only a few carefully selected synchronizer modules that are manually placed in the design
- Designers must name signals that cross clock domains in such a sway that they can be identified and reviewed
- Architects must ensure that the design is constructed in such as way such that signals crossing clock domains are limited to sub-section of the design, or are in some other way contained within specific parts of the design

Even given these strict design regulations, things can and do go wrong.

For instance:

- A designer fails to realize a signal is coming from a different clock domain, so the above regulations are unintentionally violated
- A designer realizes a signal is coming from a different clock domain but chooses a synchronization scheme inappropriate for the design (e.g., using individual synchronizer bits to synchronize a databus, which results in corrupted data values in the real hardware)
- A designer identifies the CDC path, places a correct synchronizer, but fails to use it correctly (e.g., it fails to hold the incoming CDC signal stable for multiple clock cycles to allow the synchronizer to work)

Oftentimes, these sorts of problems occur not when a design is being created from scratch, but instead, when changes are made to an existing design. This is when signals are used without realizing they come from another domain, resulting CDC signals are combined into a state machine without considering the advancing/receding nature of synchronized control signals, and so on.

A manual review of the code looks at design signals to identify the sending and receiving registers and latches. It also can identify the clock signals driving these registers and assure the appropriate synchronizers are in place. Unfortunately, reviews are manual processes, prone to errors.

For example, the review can:

- Miss a signal altogether
- Identify a signal, but fail to realize it crosses to a different clock domain due to multiple fanouts, misread a sending or receiving clock signal name, etc.
- Correctly identify all CDC signals, but fail to realize there is no synchronizer in place
- Identify all CDC signals, assure all synchronizers are in place, but not realize the synchronizer is incorrect (e.g., synchronizing multiple bits of a data bus using independent synchronizers, etc)
- Identify that all CDC signals and synchronizers are correct, but miss the fact that combinational logic placed in or around the synchronizer invalidates the timing requirements of the synchronizer

If the reviewer correctly identifies all CDC signals and synchronizers, the next step is to assure they are all used correctly. In this case, the reviewer must mentally simulate the design, assuring all possible signals are advanced and receded one clock cycle across all downstream logic. This must be propagated forward in the design to assure all functionality of downstream logic always behaves correctly under these conditions. This advancing and receding will always happen as a result of correct synchronization, and cannot be designed-out of a design containing clock domain crossings. It is a by-product of the CDC synchronization.

This is typically a challenging mental process on anything but the simplest design. The results are highly dependent on the skills of the reviewer. The possibility of making errors in this mental exercise is quite high.

Appendix B: Glossary

You may encounter these terms during DO-254/DO-178B projects. A full listing of FAA acronyms can be found at:
http://www.gps.tc.faa.gov/glossary.html

AC – Advisory Circular, such as AC-152 which enforces DO-254 for "custom micro coded devices".

ACO – Aircraft Certification Office, a local office of the FAA that assists with design approval and certificate management; US production approvals; engineering and analysis questions; investigating and reporting aircraft accidents, incidents and service difficulties; DER oversight.

AIR – AIRcraft certification service. There are various divisions of the FAA, such as AIR 120 and AIR 200, which are all involved in various aspects of aircraft certification.

AMOC – Acceptable Means of Compliance, for example, code coverage is an AMOC for verification metrics.

AOPA – Aircraft Operators and Pilots Association.

ARINC – Aeronautical Radio Incorporated, a company that is the leading provider of transportation communications and systems engineering solutions for five major industries: aviation, airports, defense, government and transportation, also synonymous with various ARINC parts such as the ARINC 429, a two-wire data bus that is application-specific for commercial and transport aircraft.

ARP – Aerospace Recommended Practice, for example ARP 5754 "Guidance for Development Validation and Verification of Complex Aircraft Systems".

CAST – Certification Authorities Software Team, an international group of participants from worldwide aviation certification authorities including the FAA, despite the name this group discusses complex electronic hardware issues also.

CEH – Complex Electronic Hardware, for the context of DO-254, this means custom micro coded devices (PLD, FPGA, ASIC).

CFAR – Code of Federal Aviation Regulations.

CFR – Code of Federal Regulations, such as CFR § 183.29, which defines criteria for DERs.

CRI – Certification Review Item, as per EASA. Pronounced "Kree", these are requirements above and beyond DO-254/ED-80, such as the CRIs for the Airbus 380 or A400M projects.

DAL – Design Assurance Level, a safety criticality rating from level A-E, with level A/B being the most critical and requiring the most stringent DO-254/DO-178B process.

- Level A: Where a software/hardware failure would cause and or contribute to a catastrophic failure of the aircraft flight control systems
- Level B: Where a software/hardware failure would cause and or contribute to a hazardous/severe failure condition in the flight control systems
- Level C: Where a software/hardware failure would cause and or contribute to a major failure condition in the flight control systems
- Level D: Where a software/hardware failure would cause and or contribute to a minor failure condition in the flight controls systems
- Level E: Where a software/hardware failure would have no adverse effect on the aircraft or on pilot workload

DER – Designated Engineering Representative, an individual, appointed by the FAA to approve or recommend approval of technical data to the FAA. These individuals can work for a specific company (such as Boeing) or be independent consultants and serve as DERs to many other companies.

DO – Document, from RTCA.

DO-178B – Software Considerations in Airborne Systems and Equipment Certification, an aviation industry standard since 1992. A DO-178C standard is being worked on for release in 2009(?).

DO-254 – Design Assurance Guidance for Airborne Electronic Hardware, put into effect on FPGA/ASIC designs via AC 20-152 in 2005.

DO-297 – Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations.

EASA – European Aviation Safety Agency, EU counterpart of FAA, pronounced "ee ah sa".

ED-12 – EU equivalent of DO-178B.

ED-80 – EU equivalent of RTCA/DO-254.

EUROCAE – European Organization for Civil Aviation Equipment, equivalent of RTCA in the US, pronounced "Euro Kay".

FAA – Federal Aviation Administration, the US authority governing aviation.

FAR – Federal Aviation Regulation, a set of requirements (US) that determines airworthiness of an aircraft. For example, large aircraft are subject to FAR 25 certification. See also JAR.

HDP – Hardware Development Plan, one of the 5 plans required for DO-254.

HVP – Hardware Verification Plan, one of the 5 plans required for DO-254.

IMA, IMS – Integrated modular avionics, integrated modular systems, DO-297 deals with this level of design.

IP – besides the traditional meaning (i.e., "intellectual property"), can also mean Issue Paper, a paper supplementing an FAA standard to clarify a problem, solution or issue not well defined within a standard.

JAR – Joint Airworthiness Requirements, , a set of requirements (EU) that determines airworthiness of an aircraft. For example, large aircraft are subject to JAR 25 certification. See also FAR.

JPDO – Joint Planning and Development Office, established to facilitate NextGen (Next Generation Air Transportation System, refers to a wide-ranging initiative to transform the air traffic control system) activities. JPDO is working with the FAA, NASA, the Departments of Transportation, Defense, Homeland Security, Commerce and the White House Office of Science and Technology Policy.

LOFI – Level of FAA involvement example LOFI on CEH projects. This is a defined evaluation criteria for establishing how much FAA involvement there should be for a given software program (See Order 8110.49). There is currently no LOFI determination for CEH/DO-254, this may be part of the draft Order 8110.CEH currently being working on.

MASPS – Minimum Aviation System Performance Specifications, for example an FAA MASPS specifies that weather information for the local region (50 miles radius or more) is continuously transmitted at least every five minutes.

NASA – National Aeronautics & Space Administration.

NextGen – NEXT GENeration air transportation system, a project to integration aircraft, airports and air traffic control to accommodate much higher volumes of air travelers/traffic in the future.

Order – An Order is a way for the FAA to address regulatory concerns in a quick but global way. Regulatory changes to the CFARs (code of Federal Aviation Regulations) take a long time and have to go through lots of steps. An Order has a specific impact to a smaller audience and is used for changes to a technology area or specific topic. Example Order 8110.CEH.

PHAC – Plan for Hardware Aspects of Certification, the main plan document required by DO-254. The other plans include Quality Assurance Plan, Configuration Management Plan, Hardware Development Plan, Hardware Verification Plan and Hardware Standards.

PSAC – Plan for Software Aspects of Certification, the main plan document required by DO-178B.

RMA – Rate Monotonic Analysis is a simple, practical mathematically sound way to guarantee schedulability in real-time systems.

RTCA – Radio Technical Committee on Aeronautics, a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance and air traffic management (CNS/ATM) system issues. RTCA functions as a Federal Advisory Committee. Its recommendations are used by the Federal Aviation Administration (FAA) as the basis for policy, program and regulatory decisions and by the private sector as the basis for development, investment and other business decisions.

SAE – Society of Automotive engineers, some subset of this group specializes in aeronautics.

SARP – Standards and Recommended Practices.

SC – Special Committee, anything that starts with SC is an industry working committee to discuss and resolve particular issues. Examples include SC-180 CEH (wrote the DO-254 standard), SC-200 integrated modular avionics, SC-205 software for aeronautical use. See also WG.

SOI 1-4 – Stage of Involvement, one of 4 required review points between a HW/SW vendor and certification authority during the DO-178B or DO-254 process.

Space Partitioning – Using the hardware MMU to enforce software partitioning of data and instruction regions in memory.

STC or Supplemental Type Certificate – Granted by the FAA for new equipment in a specific aircraft. See also TC.

Time Partitioning – Using an operating system's scheduler to ensure that selected tasks and processes have access to the CPU for a specified amount of time within a specific period.

TC or Type Certificate – Granted by the FAA to certify an entire aircraft. See also STC.

TSO or Technical Standard Order – Governs the minimum performance standard for materials, parts and appliances on civil aircraft.

UAS – Unmanned Aircraft Standards, DO-304, guidance just produced by SC-203 and being considered by FAA. Requires both DO-254 and DO-178B certification.

V&V – Validation and verification.

WG – Working Group from EuroCAE, the EU equivalent of the US-based SC (special committees, oftentimes linked directly to these activities, examples wG-72 is leading the effort on aeronautical systems security, WG-71 = SC-205.

STC – Supplemental Type Certificate, a document issued by the Federal Aviation Administration approving a product (aircraft, engine, or propeller) modification.

TC – Type certification.

TSO – Technical Standard Order, a minimum performance standard issued by the FAA for specified materials, parts, processes and appliances used on civil aircraft. A manual review of the code looks at design signals to identify the sending and receiving registers and latches. It also can identify the clock signals driving these registers and assure the appropriate synchronizers are in place.

Siemens Digital Industries Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

About Siemens Digital Industries Software

Siemens Digital Industries Software is driving transformation to enable a digital enterprise where engineering, manufacturing and electronics design meet tomorrow. The Xcelerator portfolio helps companies of all sizes create and leverage digital twins that provide organizations with new insights, opportunities and levels of automation to drive innovation. For more information on Siemens Digital Industries Software products and services, visit siemens.com/software or follow us on LinkedIn, Twitter, Facebook and Instagram. Siemens Digital Industries Software – Where today meets tomorrow.

siemens.com/eda

82184-C3 5/20 N/TGB