Insight EDA Inc
www.InsightEDA.com

Finding Leakage Cases Between Power Domains

Insight EDA, Inc

January 6, 2022

There are many forms of leakage in semiconductors. One especially nefarious type of leakage happens between power rails or power domains. The problem occurs when a DC path is formed between two power rails, either at different voltages, or when one rail is off. The DC path can involve parasitic body diodes, power switches with faulty logic controls, transmission gates, or other circuit elements.

This "inter-domain leakage" is a classic weakness of simulation, but also vitally important to find, especially in mixed power system design. In the past, designers would use a technique of chopping up supply nets with monitor resistors to track down where the leakage current was flowing.

The difficulty of finding this form of leakage has serious consequences from a CAD perspective. Traditional ERC software reports many "don’t-care" results, because it is difficult to distinguish true leakage risks. Figure 1, below, shows a classic "don’t-care" result that frequently gets reported in ERC software. As circuit size increases, more false violations will be reported, but at the same time, the risk and consequences to the circuit also increase.

The Insight Analyzer software identifies the risk of leakage between power domains, and many other issues, using intelligent heuristic algorithms that are superior to both simulation and traditional ERC.

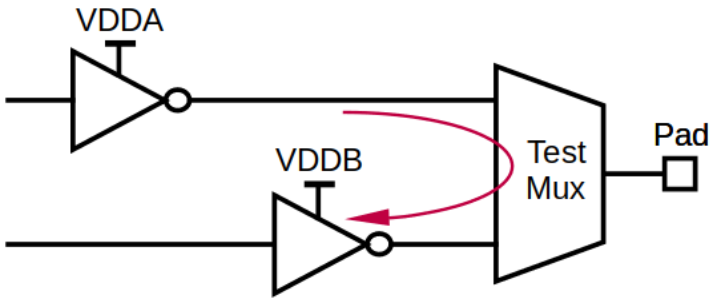

Figure 1: Test multiplexers are a common source of false violations in traditional ERC checks.

Complexities of the Problem

Before exploring a solution, it is important to understand the many different complexities that contribute to the risk of power domain leakage:

- Power rails can be described as either *internal* as a switched product, or *external* as raw power coming into the chip. This also relates to the boundaries of the device-under-test and the testbench.
- The values of power rails can be a fixed voltage, a range of voltages, or possibly switched off. Note that "off" is different from "zero volts:" a 0V rail still acts as a voltage source, whereas an "off" supply doesn't source or sink current, and can have its voltage affected by adjacent nets. Figure 2 below shows leakage from an "off" rail to an "on" rail.
- UPF states describe the values, states, and connections for power rails, switches, and isolation. A circuit design can be checked in software either with or without accompanying UPF documentation. UPF can eliminate false positives, for example, by forcing two power rails to track at the same voltage. In other words, checking a circuit without its UPF documentation may yield many false positives that would be eliminated by taking the UPF into consideration.

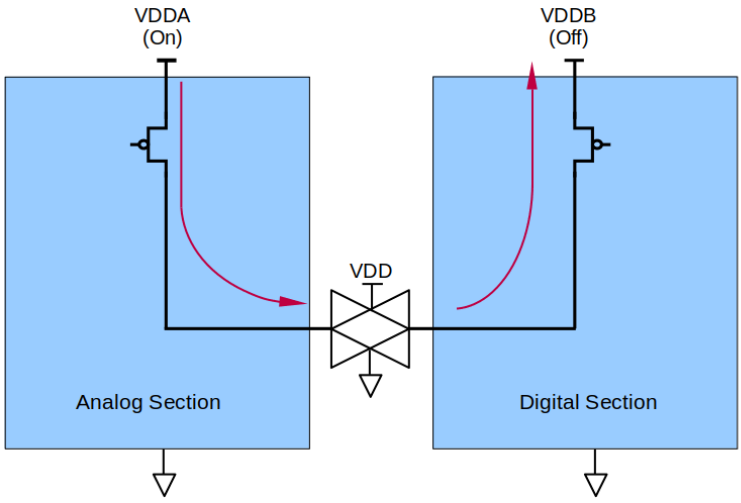

Figure 2: An example of inter-domain leakage from an "on" domain into an "off" domain.

As circuit size increases, complexity and risk also increase. This trend is shown in Figure 3, below. With traditional ERC software, the increased circuit size yields an increased number of "don't-care" results. These results are valid situations that don't pose a risk of inter-domain leakage, but still get caught by ERC and must be manually checked by the user.

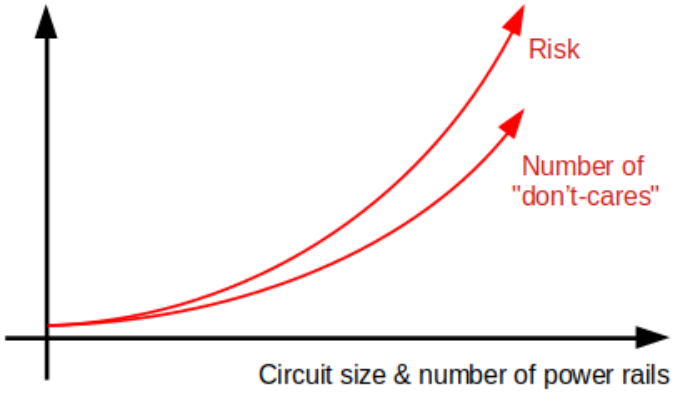

Figure 3: As circuit size and number of power rails increases, so does complexity, leading to more risk and more "don't-care" results in circuit checking scans.

Optimal Approach

The optimal approach is to first find all DC paths between power domains, based on parasitic diodes. Then, reduce the results to only the real problems and eliminate the "don't-care" results.

Finding all DC paths between power domains in the first step is relatively simple, and can be accomplished by many software packages. Reducing the results is more difficult, and requires a higher level of complexity than simply "X is connected to Y". Ultimately, the goal is to reduce the number of results to be easily checked by the end user. There are several methods to reduce the results, including:

1. UPF states: if two power rails are forced to track the same voltage, or one is always off when the other is on, then they are not a risk.

2. Controls/logic: if the "upstream" control logic ensures that two power rails will never be on together, or never be connected, then they are not a risk. For example, the mux decoder in Figure 1 is a classic "don't-care" result. The mux will only ever connect one domain at a time to the pad, so VDDA and VDDB will never have a DC path.

3. Group similar: to easily filter results and eliminate any remaining "don't-cares", the software can identify similarities between multiple result items, and group them. For example, all the results passing through the test mux would have a common instance in the leakage path, inside the mux. They could be grouped together so that the user only needs to check this results one time to eliminate all "don't-cares" for this mux.

Checking for leakage with Insight Analyzer

The problem of power domain leakage can be viewed from multiple perspectives. Depending on the type of problem, and the circuit structures involved, it might be easily caught from one angle but invisible from another angle. Insight has more than two dozen checks for circuit issues including floats, ESD, over-voltage, and many other circuit issues that can't always be caught by simulation. The relevant checks for leakage between power rails are *Contention* and *Domain Leakage*.

Contention looks at conflicting power switch controls. The software traces the path of the control logic "upstream" from each power switch, to determine which rails will be on, and at what voltages. Here, the point of view is the controlling logic of the switches.

Figure 4 shows a high-level view of a rail contention situation. Multiple power rails can be used to supply power to the same circuit. If their control logic is not adequately exclusive, they could be in a state where the two rails are directly connected to each other. In this case, Insight Analyzer would trace "upstream" to find the origin of the "Enable1" and "Enable2" signals, and report a violation if there is any chance they could both turn on together.

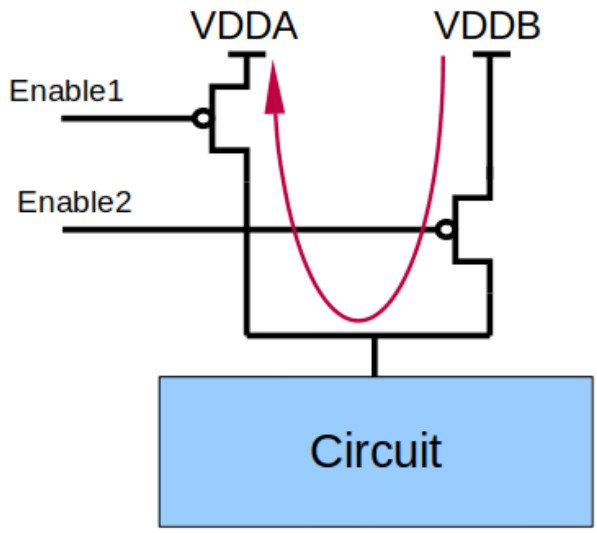

Figure 4: An example of power rail contention. VDDA and VDDB both supply power to the circuit, but if their enable signals can be switched on together, a direct path forms between the rails.

Domain Leakage looks for parasitic body diodes that could be the root cause of a leakage current, where current from one rail may sink into another rail that is off or at lower voltage. The Domain Leakage check uses an intelligent "broad scattering" approach to follow all possible unique paths the leakage current could take, without being redundant.

Figure 5 shows a situation that is reported by the Domain Leakage check. The Insight Analyzer issues a very specific violation, including: the name of the passgate instance, all steps in the leakage path, voltage values, and power states (if applicable).

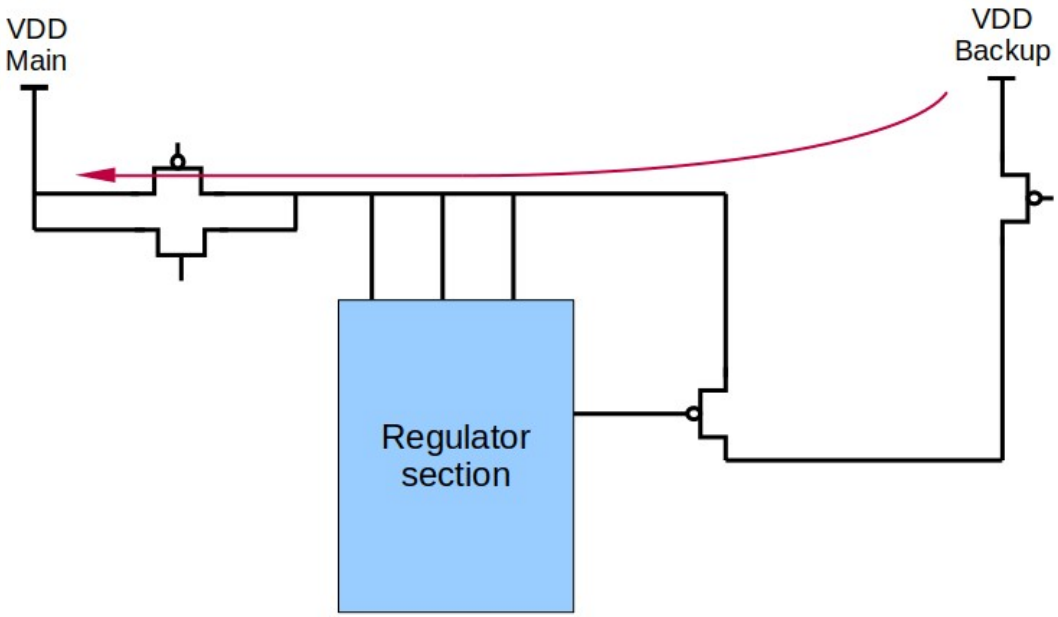

Figure 5: Another example of inter-domain leakage where a backup power supply powers into a main supply that is turned off.

Contention and Domain Leakage are both "scans" or "plugins," which scan the circuit, and report on a set of several different, but related, violations. For example, the Contention scan reports on rail contention, but also reports contention between power and ground, and "crowbar" situations.

How to Check in Insight Analyzer

The Insight Analyzer is simple to configure for inter-domain leakage by running both Contention and Domain Leakage checks. The steps below assume that preliminary setup has been done, with a netlist loaded and device parameters defined. Insight offers a plethora of

help documentation, including step-by-step tutorials, for users to reach this stage in the workflow.

1. The first step is to define power. All checks will need at least power and ground voltages to be defined. Because inter-domain leakage is more difficult to track down, it requires more detailed power definitions. In the Insight Analyzer, power states can be added, to specify which rails are on or off, and which IO signals are associated with which rails. The IO signals can also be given their own conditions in different states; for example, a state in which the "Low Voltage" rail is off, and the "Chip OK" signal is low. If a UPF file is available, it can be loaded, and parsed by the software, to automatically streamline the process.

2. Next, configure and run a "Domain Leakage" check. One important configuration option is to enable "Check rail contention", which will look for cases where multiple supply rails can be driven onto a contented node. There are other options to enable checking of certain devices or situations, and there are thresholds that determine the cutoff for what is considered a violation. More globally, there is also a slider to set the balance of "strict" as opposed to "fast".

3. Finally, run a "Contention" check with the "Rail Contention" option enabled. A part of the contention checks are dedicated to Rail Contention, where a rail type net is pulled up by multiple power switches to other rails. If the controls for those power switches have overlapping states, this is considered to be "Rail Contention". This option enables the reporting of the rail contention violation. This is slightly different from the similar-sounding "check rail contention" option in Domain Leakage, in step 2, because it looks for multiple PMOS pull-up paths to different power rails.

Interpreting Results and Fixing Inter-Domain Leakage

Both the Domain Leakage and Contention checks should be used together to fully understand the risk of inter-domain leakage for a given circuit.

The Domain Leakage check has three different types of violations that it reports, depending on the situation: "leakage into off domain," "leakage into low-voltage domain," and "leakage through ESD clamps". This scan looks for diodes that provide a leakage path from a positive current source into a current sink at a lower value. An excellent example of this type of leakage is shown above, in Figure 2.

When running the Contention check, "Rail Contention" is the relevant violation to look for. Contention is a versatile check which also reports many other circuit issues, such as shorts and ‘crowbars’. The "Rail Contention" violation is a specific sub-set of these, where the short is happening between two different rails, instead of, for example, power and ground. The

specific conditions for this violation are: A connecting bridge is formed between different supply rails with at least two PMOS FETs, not part of a power selector.

The Insight Analyzer offers many ways to view and interpret results, such as waivers, filters, gray- and black-boxing. Individual results show the full hierarchy path to the offending net or instance, which can be cross-probed and quickly viewed in schematic capture software. All violations are shown in a table in the Insight GUI which can be filtered and sorted; for example, when viewing the results of the Contention check, the user can sort all of the "rail contention" results to the top of the list.

Ultimately it is up to the circuit designer to fix the issues shown by Insight Analyzer or any ERC software. The solution could be as simple as adding a cutoff switch or changing a control signal; or it could be as complex as re-designing areas of the circuit. Insight Analyzer makes fixing the issues as easy as possible, by showing exactly what the issue is, where it is, and how it would happen.

Conclusion

As semiconductor technology continues to grow in complexity and shrink in size, leakage will be an ever-present problem for circuit designers. Many leakage issues cannot be caught by simulation or by a human-driven analysis of a circuit. Inter-domain leakage, between different power domains, will be especially challenging. Insight Analyzer has two scans in its library of circuit checks, called "Contention" and "Domain Leakage", which are specifically designed to check for inter-domain leakage.

Insight Analyzer is a full-chip, transistor-level circuit analysis tool created by Insight EDA, Inc. It is used by the world’s largest IC design houses and foundries. For more information, visit insighteda.com.