An Automated Tool for Minimizing Product Failures Due to Parasitic BJTs and SCRs

Radu Secareanu (1), Craig Johnson (2), Michael Stockinger (2)

(1) NXP Semiconductors, 2108 East Elliot Rd, Tempe, AZ 85284, USA
tel.: +1-480-413-6153, e-mail: radu.secareanu@nxp.com

(2) NXP Semiconductors, 6501 William Cannon Drive West, Austin, TX 78735, USA

Abstract - A comprehensive methodology to locate and report parasitic BJTs and SCRs that are at risk of turning on due to transient events is described. The intuitive, DRC-like implementation identifies parasitic devices classified per their risk level, offering the opportunity to fix potential design issues during the design cycle.

I. Introduction

Parasitic bipolar junction transistor ("BJTs"), either as stand-alone devices or in combined form as silicon-controlled rectifiers ("SCRs"), occur naturally in CMOS bulk technologies [1,2]. Such parasitics may be the cause of catastrophic failures in aggressive environments such as automotive applications, appliances, thermostats, power meters and motor controls. Further, such parasitics can induce functional disturbances (not necessarily catastrophic failures) in an even wider range of applications, expanding therefore the importance of controlling such parasitics in an application.

Any three active regions ("shapes") of alternating N and P types within a confined space create a parasitic BJT (Fig. 1), and any such four shapes create a parasitic SCR (Fig. 2). In case of an NPN, for example, any N shape (such as an Nwell or an N+ in Pwell) could be an emitter or collector, and any P+ in Pwell could be a base. Furthermore, Pwells and Nwells may belong to various process

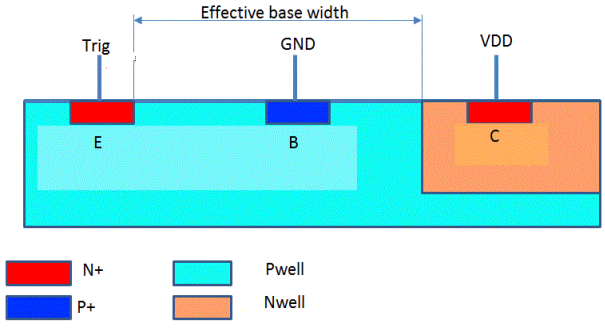

Figure 2: Example of a stand-alone parasitic BJT (NPN depicted)

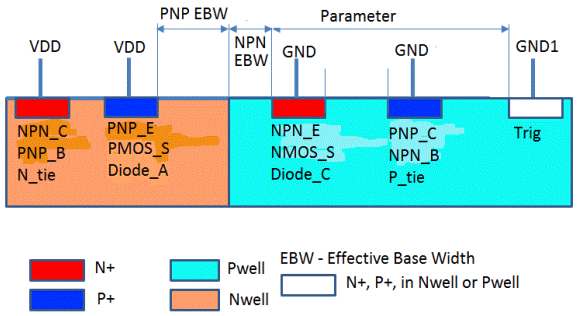

Figure 1: Example of a parasitic NPN/PNP pair forming an SCR

modules (for example low-voltage or high-voltage), and the N+ in Pwell could be the cathode of a diode or the source/drain of an NMOS device.

In a real chip, there may be millions of parasitic BJT and SCR devices. However, typically only a few are considered "risky", meaning that they could turn-on and interfere with normal chip operation because of a transient event, such as an ESD or EFT (Electrical Fast Transient) event. The rest of the devices are "dormant" (perhaps 99.99% or more).

Consequently, the process of correctly and automatically selecting just this very small percentage of parasitics that can represent a risk, is very complex [3-7]. In this paper, a comprehensive automated methodology to locate, characterize, and report these risky parasitics is described. The methodology is implemented as a DRC-like checker, taking a physical design view as an input and flagging risky parasitic devices to the designer. Automated full-chip analysis can be achieved in "minutes-to-hours" run time.

II. Methodology Implementation

A. Top-level Tool Overview

A top-level overview of the tool flow is provided in Fig.3. The input is a physical design database (e.g. in GDSII format). During database preparation, all power (VDD), ground (GND), and external IO nodes need to be labeled at the top level of the layout view ("connectivity"). A GUI ("Interface") allows the user to select the analysis target and to modify a set of geometry parameters that impact the search procedure (see section II-B). Then the tool performs the following key steps listed below, without further user interaction. It utilizes Calibre® PERC™ LDL for the first step (searching for parasitic BJTs). The "engine" used for the remaining steps uses custom C++ code, proprietary to our checking tool.

a. A set of search recipes is used to locate risky parasitic NPNs and PNPs. The recipes use geometry parameters from the GUI, connectivity information from the database, and several other criteria (described later in section II-B).
b. SPICE models can be created based on technology characterization of parasitic devices (section II-C).
c. Individual parasitic NPNs and PNPs are matched into SCRs. These SCRs and non-matched BJTs are being classified based on impact and risk (section III).
d. Risky parasitic devices are reported and visualized (section III).
e. SPICE models of reported devices can be back-annotated in the original schematic for impact simulations.

B. Criteria for Risky Parasitic Devices

To identify risky parasitic devices, this tool employs a set of complex criteria, which are described next. These criteria together are used to discard most dormant parasitic devices.

Connectivity

The general SCR of Fig. 4 is used to explain connectivity criteria. This SCR has four terminals,

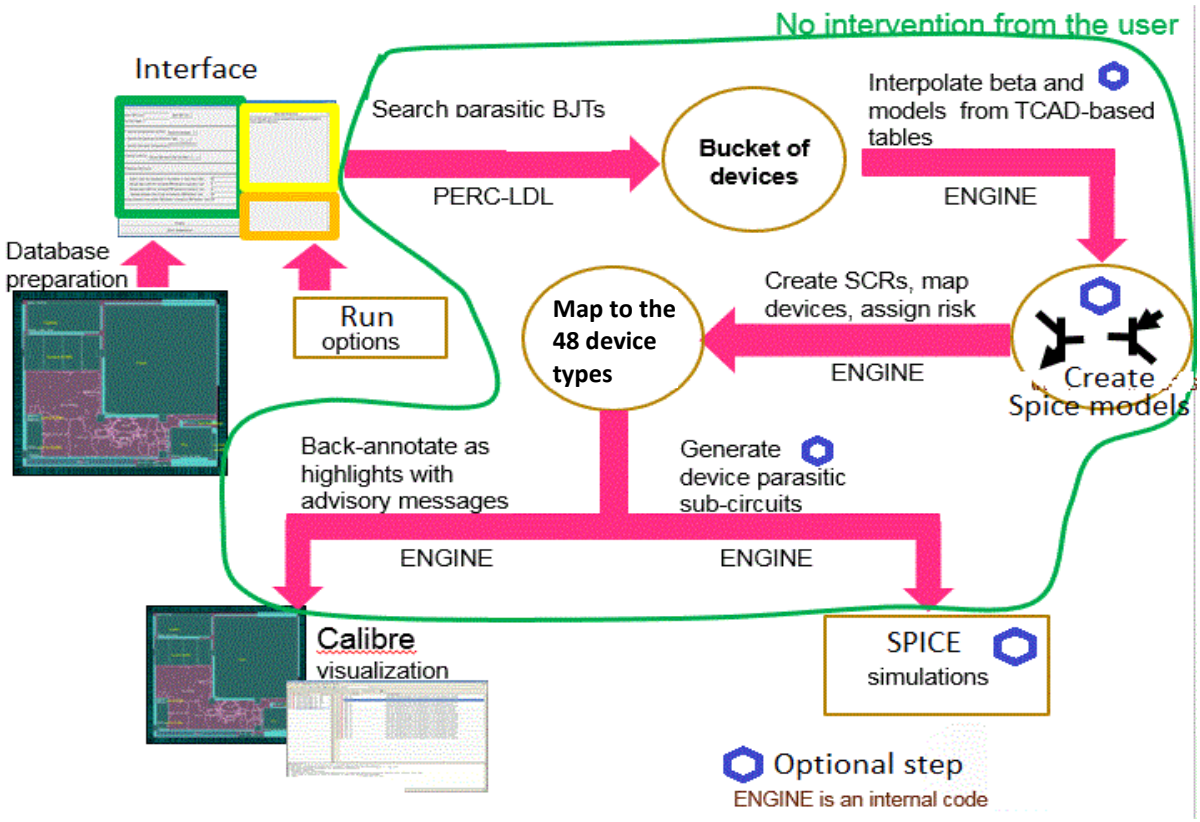

Figure 3: Tool flow overview

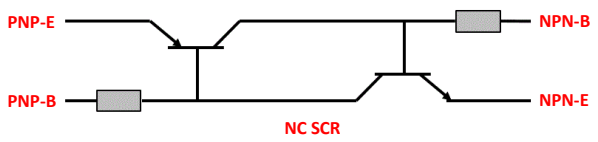

Figure 4: General "non-defined connectivity" (NC) SCR

NPN-E, NPN-B (merged with PNP-C), PNP-B (merged with NNP-C), and PNP-E. As previously described, any of these terminals may connect to nets labeled as GND, VDD, or IO. Otherwise, a terminal has "undefined" connectivity. Note that the defined GND and VDD nets only propagate through metal connections. IO nets propagate through metal and through resistors of a defined maximum resistance, which is a parameter defined in the GUI.

The tool will only consider parasitic devices whose terminal connectivity could lead to a device turning on. For example, a device with NPN-E connected to GND or IO and NPN-C connected to VDD may turn on, whereas a device with NPN-E connected to VDD or with undefined NPN-E connectivity (e.g. an internal node) may not. The latter is only true if the internal node could not sink enough current to sustain parasitic NPN conduction. Otherwise (e.g. for an on-chip regulated GND supply) the node should be labeled as a GND net. This distinction needs to be made by the user. Similar criteria are also applied to PNP devices.

Trigger domains

To further narrow down the search for risky devices, identifying "trigger domains" is key. Consider, for example, the SCR of Fig.4 with NPN-E and NPN-B connected to GND, and PNP-E and PNP-B connected to VDD. Such a two-terminal SCR would meet the above connectivity criteria, but it may still not be at risk of triggering unless there were an "aggressor" nearby. The chip core ("sea of gates") typically contains millions of such SCR devices. The trigger domain criterion adds the requirement that a qualifying substrate current injector must exist within a certain radius from a parasitic device. This injected current may forward-bias the B-E junctions of the NPN or PNP devices. Examples of aggressors include a second substrate GND domain (different from the NPN-B) or a diffusion region (N or P) that is tied to an IO.

Other "trigger domain" criteria apply to three or four-terminal SCRs. For example, if the NPN-E and NPN-B connected to different GND nets or if any of the terminals connected to an IO, they would also be considered risky devices.

Geometry criteria

As mentioned, any parasitic device is composed of three or four shapes. The distance between these shapes and their sizes represent important geometry criteria used by the tool. All shapes must be in a confined space for parasitic BJTs or SCRs to be considered risky devices. Several examples follow.

An SCR may turn on only if its loop gain ($\beta\_NPN*\beta\_PNP$) is greater than 1. The β of a BJT depends on the effective base width. Therefore the tool will only report devices where the E-C distance is greater than a pre-defined parameter set by the user in the GUI (see section II-A).

Another geometry parameter is the distance between the effective base region of a BJT and the base contact. A larger distance means a greater effective base resistance and therefore a smaller amount of substrate current required to turn-on the BJT. The sizes of the constituent shapes are also important geometry criteria. E.g. a small emitter area means small current and therefore a relatively low risk of turning on an SCR.

Technology-specific default geometry parameters, determined using TCAD and/or measured data (section II-C), are available in the GUI. The user can increase parameters (get a more comprehensive risky device coverage) or reduce parameters (get a more selective coverage). As discussed in section II-C, though geometry parameters are sufficient to run the tool, technology characterization is key in defining these parameters.

Search criteria

Recognizing all possible risky BJT and SCR devices as a function of so many criteria would require a large collection of device "recipes" (see step "a" in section II-A). Since fewer recipes translate into improved efficiency (i.e. shorter run times), several methodology features have been implemented based on certain key observations. For example, in an SCR, the NPN collector and PNP base shapes must be merged, and the NPN base and PNP collector shapes must be merged. Therefore, the general search algorithm for parasitic devices can be comprised of searching for parasitic NPN and PNP devices only. Then, to find and report parasitic SCRs, a "matching algorithm" searches

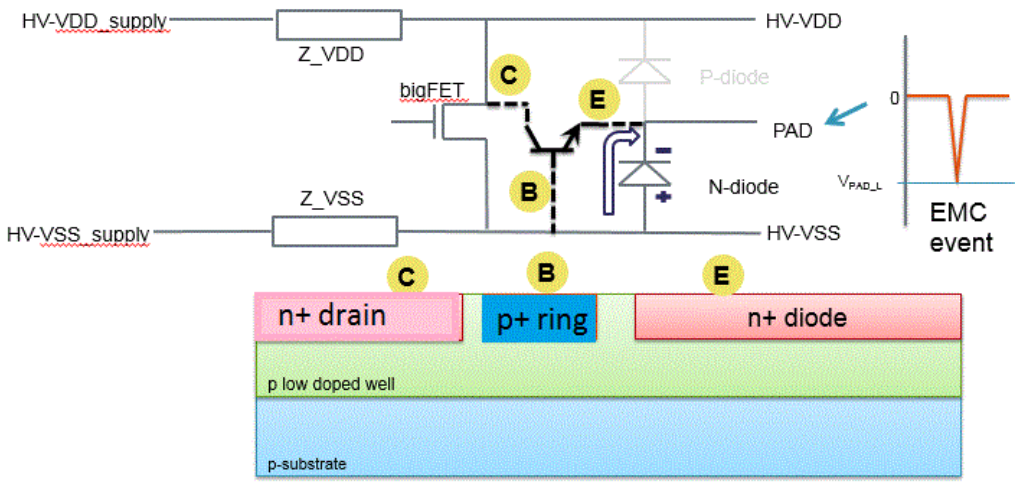

Figure 5: Example of a damaging stand-alone parasitic NPN

through all located NPNs and PNPs and checks for the base-collector pair requirement. Risky NPN and PNP devices that remain stand-alone (i.e. not part of any SCR), will be classified as such. Note that these stand-alone parasitic BJTs may also be at high risk of damage, as shown in the example of Fig.5.

In this structure, the NPN-E is the cathode of an ESD protection diode inside an IO pad cell, the NPN-B is a substrate contact, and the NPN-C is the drain of an NMOS clamping device (bigFET). When the NPN is turned on due to a transient event on the IO pad (diode cathode), the high collector current on the NMOS drain could damage the NMOS device.

Searching only for NPNs and PNPs turns out to be a fundamental aspect of our methodology. Besides the clear advantage of simplifying the search algorithm for finding a multitude of stand-alone NPNs, PNPs, and SCRs, it allows for the characterization of parasitic devices in terms of gain (β) and relative magnitude of emitter, base, and collector currents (as explained in section II-C).

C. The Technology Component

The manufacturing technology has a key role in differentiating which parasitic devices are reported as risky. For example, technology characteristics impact parasitic well resistances and bipolar gains [8]. The discerning geometry parameters used by the tool (section II-B) strongly depend on technology options such as the presence of deep Nwell (DNW) or the types of wells involved (e.g. a HV well with lower doping versus a LV well with higher doping). Therefore, technology aspects are deeply embedded in the decision-making process of the tool.

To inherently include such technology aspects, this tool offers the capability to model parasitic NPN and PNP devices. This occurs in several steps. Given a located parasitic BJT, all its physical dimensions pertinent to the three (E, B, C) constituent shapes, such as width, length, and distances between shapes, are extracted from layout. Based on these numbers, a parasitic device (SPICE) model is interpolated from look-up tables, which have been generated using TCAD as part of a technology characterization step. The tables contain a representative coverage of parasitic devices of the technology, with practical size sweeps and well type combinations that may occur.

Note that this technology characterization serves two purposes. The first (main) purpose is to assess the risk of parasitic devices, as described in section II. If parasitic SPICE models are available, they are used directly by the tool to make this risk assessment. Otherwise the geometry parameters entered in the GUI (see section II-A) are used, and technology aspects may only be used as an aid in setting these parameters.

The second purpose is the creation of parasitic device (SPICE) models and back-annotating them in the original design schematic (see steps “b” and “e” in section II-A). This step is optional as most users only need the tool to locate parasitic devices. Steps “b” and “e” may also add significantly to the

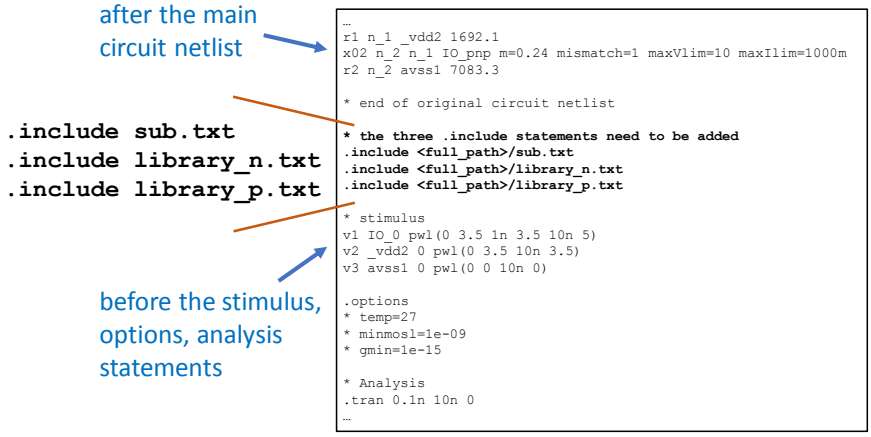

Figure 6: An example on how to use parasitic models and back-annotate in the original circuit schematic

run time of the analysis and are typically only used under special circumstances.

An example describing the use of parasitic models and back-annotation is shown in Fig.6.

For every parasitic, the tool generates from the TCAD data a unique SPICE model. This model will be written in library_n.txt file (NPN) or library_p.txt (PNP). The tool also writes the sub.txt file with the sub-circuits associated with the respective parasitic devices. Since all the parasitic devices have their connectivity and device information for the E, B, and C shapes associated with the original circuit, these parasitic models and sub-circuits generated by the tool can be back-annotated into the original circuit. In order to do that, the user needs to include these three files generated by the tool (as shown in Fig. 6) in the SPICE simulation test bench.

D. Further Run Time Improvements

One way of further minimizing run time is to tightly limit the search to areas of a particular concern, e.g. near selected triggers (aggressors). This can be done by defining a circular area with radius R around the aggressor and excluding the rest of the chip from the search. Examples include overlapping GND1 and GND2 domains (both tapping onto the substrate) and shapes that connect to external IO pads.

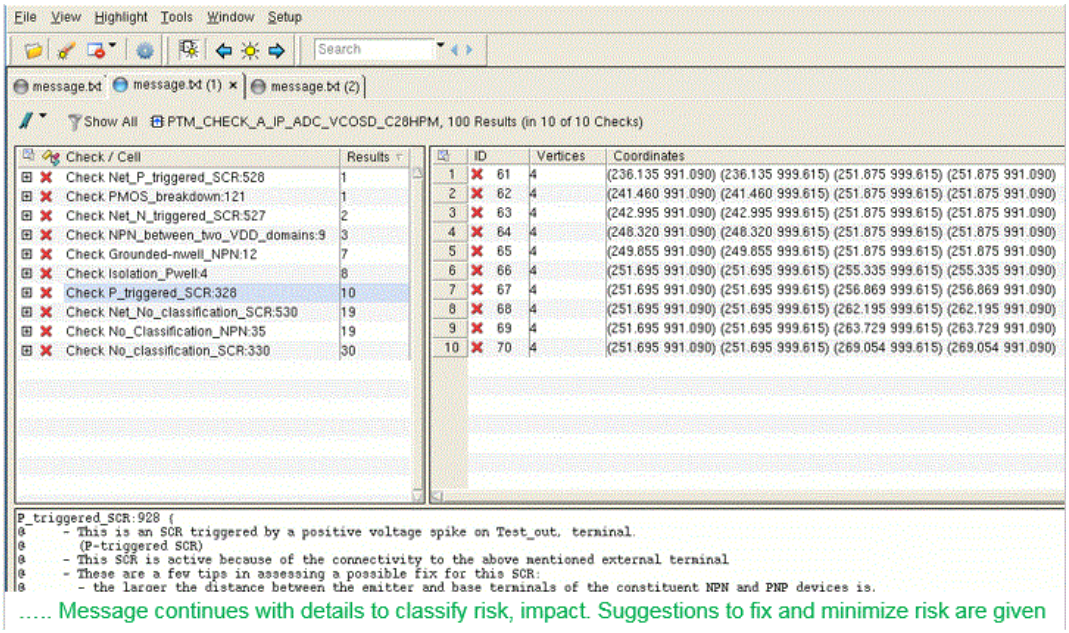

Figure 7: Report window for the type of parasitic found in a design

These and several other criteria implemented in the tool to limit search areas enable full-scale chip analysis within several minutes (for circuit blocks) to several hours (for large microcontrollers).

III. Reporting

Our tool has been implemented in an easy-to-use integrated package, which can be run like a DRC check. Upon completion of an analysis, the resulting risky devices ("flags") are being reported for further investigation by the designer. These flags are cross-referenced with the layout and are accompanied by explanatory messages, as exemplified in Figs. 7, 8, and 9.

While all flagged parasitic devices generally pose a risk of turning on during circuit operation, this may not hold true for a specific usage scenario. For example, there could be an off-chip decoupling capacitor or dedicated protection device connected to an external IO pad, which is considered a "trigger" (aggressor) in our search methodology. This configuration may limit the propagation of a transient event from the IO pad into the chip and may thus diminish the risk of certain flagged devices [9]. Accordingly, the designer running the analysis, knowledgeable of such design details, has the option to fix certain flags that truly pose a risk and to "archive" remaining flags for reference, in case an issue comes up later during the testing or operation of the chip. This may speed up the root cause analysis and the search for a fix later.

The reported parasitic devices are classified based on their potential design impact, risk, and meaning. Currently, 48 parasitic device types can be reported

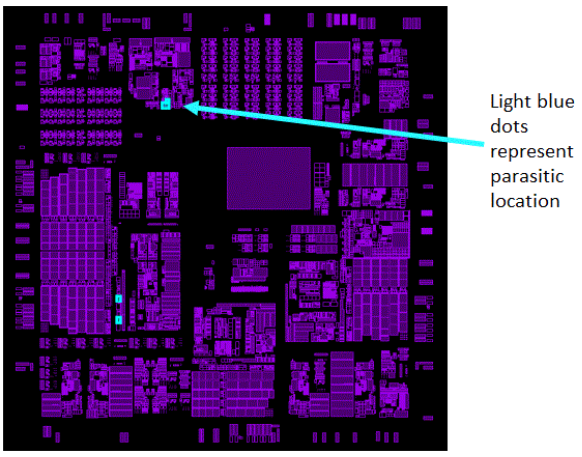

Figure 8: The flags specific to one type of parasitic device are being highlighted in the layout database

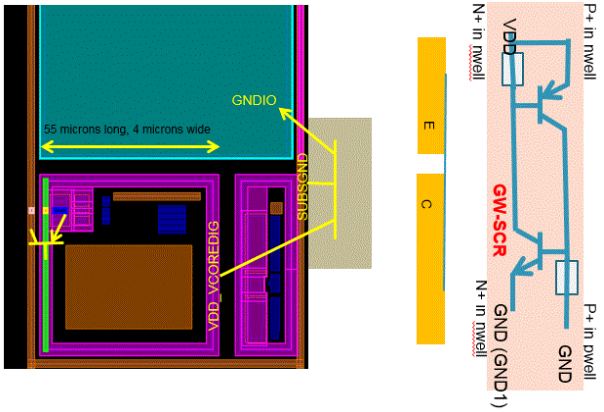

Figure 9: For every parasitic BJT, the user can highlight the related E, B, C shapes. In this example of a Grounded Nwell SCR, the NPN and PNP shapes of the SCR are shown.

(Fig. 10 illustrates these 48 types). This device type classification provides a clear insight into the potential trigger mechanism and helps a designer minimize the associated risk. Providing all details of the 48 device types is beyond the scope of this paper, but some aspects will be discussed.

For example, the "breakdown" NPN or PNP type can cause damage to the drain (collector of the BJT) of an active MOS device. The "substrate bias" NPN type relates to the fact that such a device may create a significant unwanted body bias for active devices, e.g. due to a low density of substrate ties. The "power-domain conflict" NPN type implies that there are two VDD domains in immediate vicinity - this could lead to problems if the difference between the two VDD levels is large.

The 15 SCR types are classified based on the connectivity of the four terminals (section II-B), on the location and nature of any nearby substrate current injector, and on the nature of the wells that build the SCR. For example, a two-terminal SCR as described in section II-B is classified as "substrate triggered" because it can be triggered by a nearby substrate injection current that forward-biases the B-E junction of the constituent PNP or NPN devices. An SCR that has its NPN-E as a grounded Nwell is classified as a "grounded-Nwell SCR". An SCR that has its PNP-E connected to an external IO is classified as a "p-triggered SCR". An SCR that has its NPN-B connected to a dedicated bias supply (i.e. different from the ground supply tied to NPN-E) is classified as a "p-tracking SCR". Combinations exist, such as "p-triggered, grounded Nwell SCR".

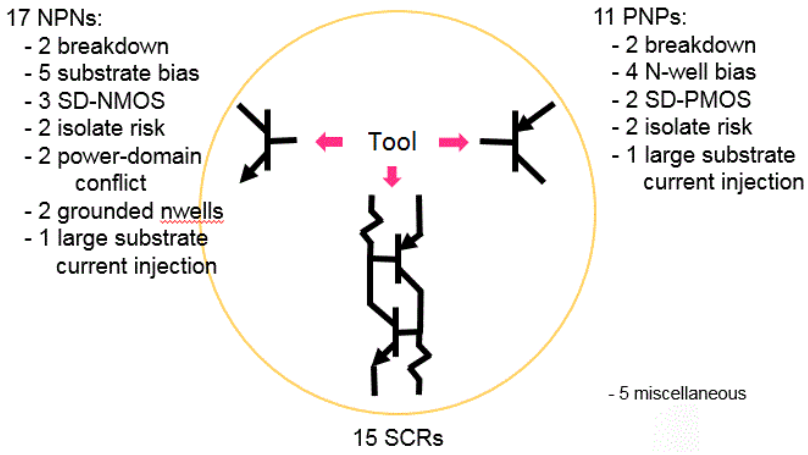

Figure 10: The range of meanings for the 48 reported parasitic types

The reporting window depicted in Fig. 7 is familiar to Calibre® users. In the left column, the flagged device types are listed, with the number of instances for each type. When a specific type is selected in the left column, all instances for that type are listed in the right column. When an instance is selected in the right column, a message with characteristic information of the instance (e.g. connectivity, technology, sizing, loop gain, beta, risk info, etc.) is displayed in the bottom section. This additional information may be useful for the designer to further understand and debug the device.

Also, when a specific type is chosen in the left column of Fig.7, the designer can display the location of all the instances (or flags) belonging to that type in the layout window, as shown in Fig.8. If the designer wants to focus on one specific instance, he or she can "zoom" into that instance and display the location of all constituent shapes in the layout view, as depicted in Fig. 9 (enhanced for understanding).

IV. Conclusions

A methodology to locate, characterize, and report risky parasitic BJTs and SCRs has been presented. The methodology can run full chip-level analysis with the ease of a DRC-like check. Due to the implemented approaches, the tool run time is highly efficient. Performing this analysis helps producing chip designs that are virtually free of risky parasitic devices, eliminating costly product failures and debug efforts.

References

1. Yoon Huh et al., "Chip Level Layout and Bias Considerations Preventing Neighboring I/O Cell Interaction-Induced Latch-up and Inter-Power Supply Latch-up in Advanced CMOS Technologies," EOS/ESD Symp., 2005, 2A.2
2. M. Stockinger et al., "Device Interactions between ESD Diodes and CMOS Clamps in CMOS Processes", EOS/ESD Symp., 2014, 5A.1
3. S. Bargstadt-Franke et al., "Transient latch-up: Experimental Analysis and Device Simulation", EOS/ESD Symp., 2003, 2A.3
4. K. Domanski et al., "Transient LU Failure Analysis of the ICs, methods of Investigation and Computer Aided Simulations", IEEE Reliability Physics Symp., 2004, pp.370-374
5. T. Smedes et al., "A DRC-based check tool for ESD layout verification", EOS/ESD Symp., 2009, 4A.2
6. T. Li et al., "Layout extraction and verification methodology for CMOS I/O circuits", DAC, 1998, pp. 291-296
7. M. Khazhinsky et al., "EDA approaches in identifying latchup risks," EOS/ESD Symp., 2016, 5B.3
8. R. Secareanu et al., "Impact of low-doped substrate areas on the reliability of circuits subject to EFT events", IEEE SOCC, 2010, pp.21-24
9. M. Scholz et al., "Impact of the on-chip and off-chip ESD protection network on transient-induced latch-up in CMOS IC", EOS/ESD Symp., 2013, 3B.3