On-chip ESD protection for Internet of Things

ON-CHIP PROTECTION

for electrostatic discharge (ESD) and electrical overstress (EOS)

On-chip ESD protection for Internet of Things

Cisco predicts that more than 50 Billion devices will be connected to internet by 2020. It is called "Internet of Things" (IoT). Many wonder how connecting your refrigerator to internet will benefit anyone. But IoT is about much more than automated shopping lists. When you combine sensors, actuators, and networked intelligence the possibilities are endless. It can boost productivity, save resources and even prevent health issues.
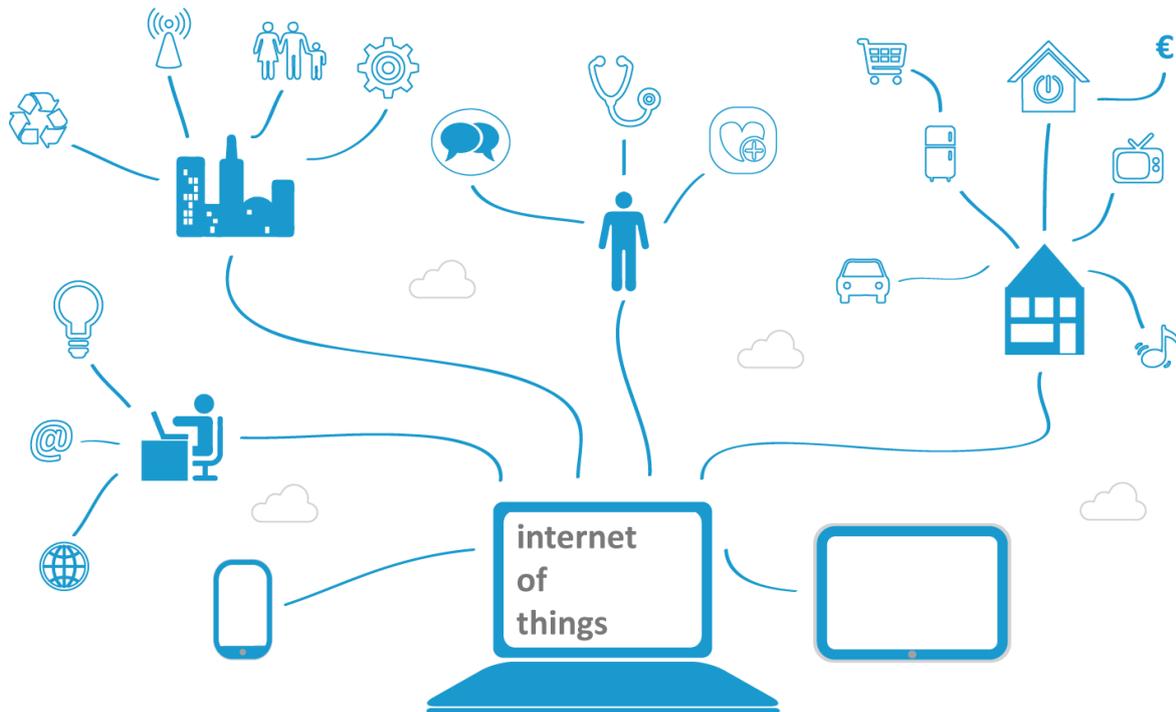
Many IoT chips can be made in older, depreciated fabrication plants (0.25um, 180nm, 130nm) that were top-notch 20 years ago. One would argue that foundries have covered every aspect of Electrostatic Discharge (ESD), Electrical Overstress (EOS) and Latch-up in these mature processes long ago. But we learned, by supporting innovative semiconductor startups, that **many of the applications in IoT require non-standard on-chip ESD protection clamps**.

1. IoT chips require special ESD protection clamps

Many of the applications in Internet of Things require non-standard on-chip ESD protection clamps. We identified 5 reasons.

Non-standard signal voltages

Several IoT systems include sensor interfaces with distinctive signal conditions (5V or even 20V), beyond the typical General Purpose I/O (GPIO) interfaces provided by the foundry. Similarly, small signals (order of a few mV or mA) captured by sensors for motion detection and touch remain hidden in the noise or are lost due to leakage from GPIOs.

Low leakage requirement

A lot of the IoT applications run on a battery or harvest energy. Designers move heaven and earth to reduce the leakage of the functional circuits. Foundries on their end provide special low-power process options to reduce both standby and dynamic power. It would be unwise to nullify all that work through the use of leaky ESD clamps.

Sub-systems are powered down

To further reduce the leakage only a small part of the system is awake all the time. All the other circuits are turned off unless required. Traditional ESD protection can ruin the efforts when signals applied on the I/O circuits power-up a functional block not required at that time.

Wireless interfaces

Every system needs to communicate. Therefore, wireless interfaces can be found on all of the IoT systems. This requires on-chip ESD protection with low parasitic capacitance.

System level protection, on the chip

A lot of the innovative systems are meant to be low-cost and mobile and also this relates to ESD. To reduce the size and the Bill of Materials (BOM), system designers remove board level ESD protection from the mini-Printed Circuit Boards (PCB). 20 years ago, such Transient Voltage Suppressors (TVS) devices were added to protect ICs against ESD stress during the actual use of products. Without such TVS protection and due to the shorter PCB traces Integrated Circuits are now stressed with more severe ESD events like IEC 61000-4-2. Moreover, the probability of ESD-stress is much higher in those mobile systems as they are operated in so-called harsh environments.

Clearly, IC designers need to think about the ESD protection strategy for their IoT system. It is wise to rely on silicon proven concepts to speed up market introduction.

The next part of the document provides solutions when the traditional ESD concepts are not sufficient.

2. Replacing the traditional ESD diodes

The 'Dual diode' approach is one of the most used on-chip and off-chip concepts for ESD protection of IO interfaces. It is simple to implement, smaller than any other IO/ESD concept, has a low parasitic capacitance and low leakage.
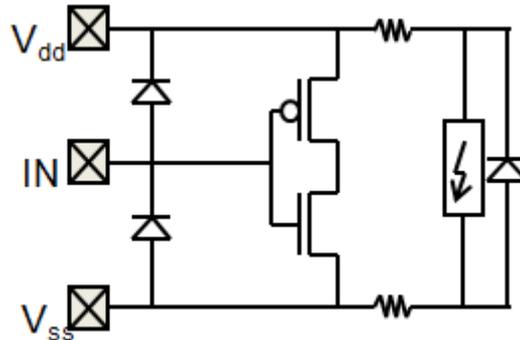
Dual diode based ESD protection concept for IOs.

However, especially the 'diode up', from IO-pad to VDD can create a lot of problems in the functional operation of Internet of Things (IoT) circuits. There are basically **3 main reasons** why the 'dual diode' concept is causing trouble.

1. The signal voltage for sensor interfaces can differ from the IC supply voltage

2. Some communication approaches require so-called "open drain" concepts

3. Sub-systems of the SoC are powered down

Fortunately, there are many different concepts that IC designers can use. Below there are 6 different concepts that can replace the dual diode protection.

Concept 1: Series connection of diodes

The most straightforward solution is to increase the number of diodes between IO-pad and VDD. The number of diodes defines the voltage level at which the forward diodes start to conduct current.
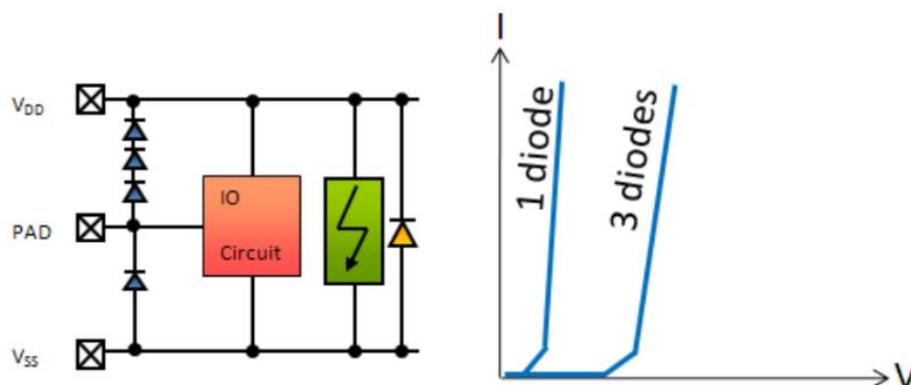

By connecting a number of diodes in series the 'diode up' issue can be easily solved for a number of cases. The amount of series connected diodes depends on the maximum voltage that the IO-pad can raise above the VDD level.

It is a simple concept within a small area and can be adapted for different voltage ranges. It actually can improve capacitive loading and can be designed for low leakage. The main drawback is that the voltage drop during ESD stress could go beyond the maximum voltage of the circuit to be protected.

Concept 2: Add a clamp from I/O to Vdd

Similar to the series diodes, the ESD designer may replace the „diode up" with a dedicated ESD clamp device. The clamp forward conduction is from IO to VDD.
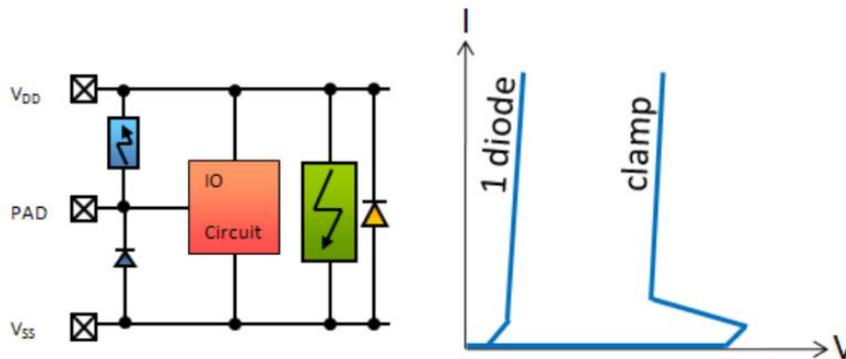

The single diode can be replaced by a dedicated clamp device.

With the right clamp design, the leakage can be low. It has some drawbacks like higher parasitic capacitance, larger area. It is also more difficult to set a specific threshold. Similar to the first concept the added voltage drop during ESD stress may be too high.

Concept 3: Use another Vdd reference

Another simple approach consists of connecting the diode from IO-pad to another voltage reference.
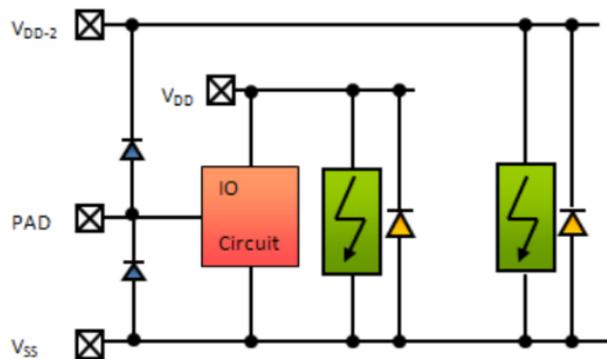

Connect the 'diode up' to another voltage domain.

This solution works only under certain conditions.

- The second domain (VDD-2) has to run at a voltage level above the maximum signal voltage on the IO-pad and must remain powered. This is a problem for failsafe, hot swap and many overvoltage tolerant cases.

- An efficient ESD protection clamp is required between the VDD and VDD-2 domains

- A strong back-end / metal connection for VDD-2 is required at the IO-pad

Concept 4: Use an internal supply, separate from the Vdd power line

Similar to concept 3 the VDD-2 could be an internal „ESD bus" only, without connecting it outside of the IC. In this concept the first constraint can be dropped: The ESD bus does not need to be powered.
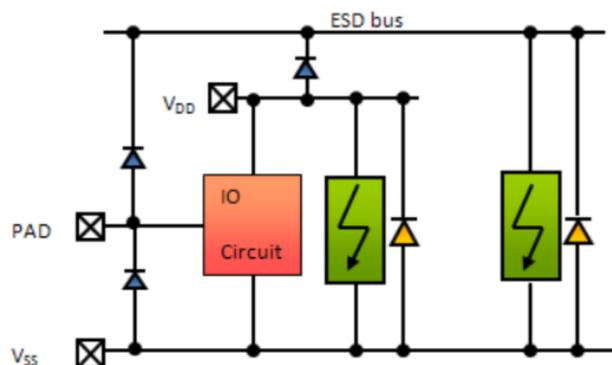

The 'diode up' can be connected to the ESD bus.
The advantage is that the ESD bus does not need to be powered.

The main drawback is the larger silicon footprint. The designer needs to add an additional power clamp and wide metal lines for the ESD-bus.

Concept 5: Self-protective drivers

Many open drain concepts rely on so-called self-protective output drivers. The ESD stress from IO-pad to Vss and from IO-pad to Vdd runs through the NMOS output driver. The MOS transistor can shunt ESD current either in active or snapback/bipolar mode.
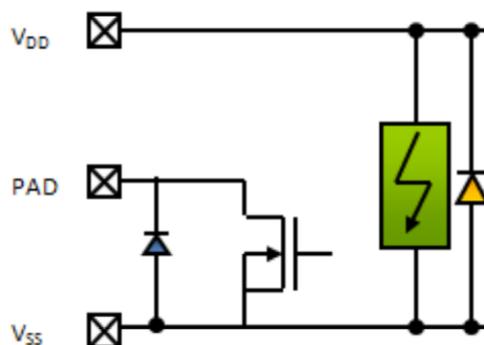

The self-protective driver acts as an ESD clamp device

The output driver is part of the functional circuit and already needs to be large to shunt large currents. It therefore feels appropriate to rely on the self-protective concept and not waste additional silicon space to include dedicated clamp elements. However, high voltage tolerant transistors tend to be easily damaged during ESD stress.

Concept 6: Local clamp between IO-pad and V$_{SS}$

It is possible to protect circuits with dedicated, local, ESD clamps in parallel with the functional circuits.
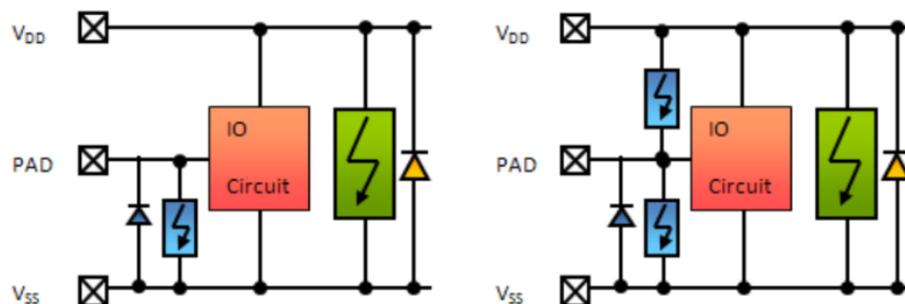
Local clamp protection concepts. In most cases the left version (clamp between IO-pad and VSS) is sufficient. However, if there is ESD sensitive circuitry between VDD and IO-pad that requires low voltage clamping then a second clamp can be added between VDD and IO-pad.

Although the silicon footprint increases this concept is very flexible because there are many clamp options available, even with low leakage and low parasitic capacitance.

„Dual diode" based ESD protection is the most used concept for IO protection. It has many benefits but can also introduce a lot of problems during functional operation of the protected circuit.

When the diode to VDD is removed to improve functional operation another ESD device or concept is required to ensure that the circuit is well protected. Various concepts are described above. The most optimal concept depends on the actual requirements. Contact us if you need help selecting the right solution for your circuit.

3. Selecting the most relevant EOS/ESD standards for IoT applications

In the Internet-of-Things (IoT), semiconductor circuits will be used in places where they have never been used before. This includes places where the harsh environment demands high reliability (automotive, industrial applications), or where replacement of the parts is impossible (like implants). IoT circuit designers are faced with the challenge of defining the reliability requirements for new applications.

Suppose the IoT application consists of a wireless button. The user can program the button to control any connected appliance. You can turn on lights, start the dishwasher, open the curtains, start the Tesla, order more toothpaste or all those things combined. The button can be glued to any type of surface, anywhere in the home, car or office. But what are realistic stress cases for the integrated circuits (IC) that are embedded in the plastic cover? What if there are no outside connections at all? How can the product designer determine the right ESD specifications for the internal ICs? Can air discharge with a zap gun be correlated to real events? How can this be included in the IC design?

Image courtesy of Idea go at FreeDigitalPhotos.net

By nature of the application, the button will be touched by human fingers often in its lifetime. Therefore, the product designer can expect many ESD events. Due to the complete encapsulation however, humans will not be able to touch the IC or any leads going to the IC.

The IEC 61000-4-2 system level ESD specification, notably the air discharge variant seems appropriate for the application. However, the plastic encapsulation determines the amount of ESD stress seen by the IC. Though no direct charge is being transferred to the IC, charge redistribution might cause ESD damage, especially in the more advanced process nodes. The difference between the air discharge specification and the real event is clearly the material the ESD stress has to travel through before reaching the leads of the IC. It has a big impact on the stress case.

Designers need to make choices, not only how to handle the ESD stress, but also what kind and how much stress is expected. In some cases, EOS events are expected, sometimes modeled similar to IEC 61000-4-5, which was intended as a lightning specification, with kA of current. The lack of a better specification forces designers to be creative in working on the reliability of their product.

Including an EOS/ESD specialist in the design team is often required to resolve the matter. In all protection choices, the specialist evaluates the stress type handled by the ESD protection. For instance, in the button example, it will be unclear what the rise time and pulse width of the real world even may be, and therefore a dynamically triggered MOSFET clamp is probably not the best option. For these uncertain stress cases, often voltage level triggered clamps are more robust. Similarly, the holding voltage of the ESD clamp should be higher than the supply level, to avoid any potential latch up or EOS failure.

4. Sofics

Sofics joined the Design Center Alliance of TSMC already in 2008 based on positive feedback from several of TSMC's customers. In 2010 Sofics joined the IP alliance partnership when TSMC licensed the Sofics PowerQubic ESD clamps for 0.25um BCD technology.

Sofics currently supports more than 40 TSMC customers, across many different nodes, applications.

Percentage of projects on TSMC technology nodes
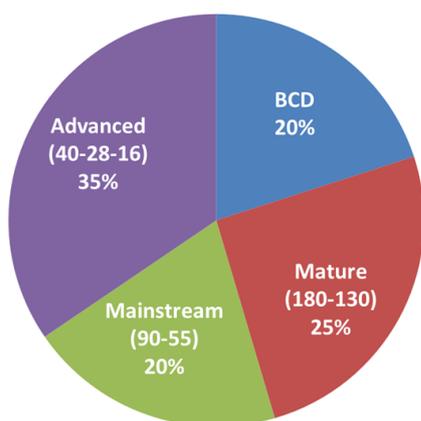
Node	Voltage domains
350nm HV	3.3V 15V
250nm BCD, gen. I and II	12V 24V 40V 60V
180nm BCD, gen. I and II	18V 24V 32V 40V 60V
180nm CMOS	1.8V 3.3V 5V
130nm CMOS	1.0V 1.2V 3.3V 5V 7V
90nm CMOS	1.2V 1.8V 3.3V
65nm CMOS	1.0V 1.2V 1.8V 2.5V 3.3V 5V
40nm CMOS	0.9V 1.2V 1.8V 3.3V 5V
28nm CMOS	0.85V 0.9V 1.8V 3.3V 5V 5.5V 12V
16nm FF+	0.8V 1.2V 1.5V 1.8V 2.5V 3.3V 5V

Sofics on-chip ESD protection library

- ESD clamp solutions across 10+ CMOS generations
- Verified in 10 foundries and 30+ fabs (foundry and proprietary)
- 3000+ IC designs supported since 2000
- 80+ customers worldwide
- Patent protected portfolio
- Reduce IC cost, pass any ESD/EOS/LU specification and enhance IC performance

5. Conclusion

Clearly, IC designers need to think about the ESD protection strategy for their IoT system. It is wise to rely on silicon proven concepts to speed up market introduction.

About Sofics

Sofics (www.sofics.com) is the world leader in on-chip ESD protection. Its patented technology is proven in more than 3000 IC designs across all major foundries and process nodes. IC companies of all sizes rely on Sofics for off the-shelf or custom-crafted solutions to protect overvoltage I/Os, other nonstandard I/Os, and high-voltage ICs, including those that require system-level protection on the chip. Sofics technology produces smaller I/Os than any generic ESD configuration. It also permits twice the IC performance in high-frequency and high-speed applications. Sofics ESD solutions and service begin where the foundry design manual ends.

Contact Sofics

Contact Sofics by email: IoT@sofics.com

Notes

As is the case with many published ESD design solutions, the techniques and protection solutions described in this report are protected by patents and patents pending and cannot be copied freely. PowerQubic, TakeCharge, and Sofics are trademarks of Sofics BVBA.

Please contact Sofics to learn about our affordable license conditions.