Volume 35, Number 5, October, 2001

Download this article in PDF format. (75 KB)

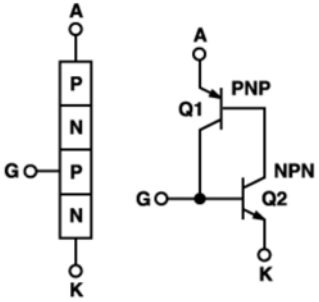
Winning the Battle Against Latchup in CMOS Analog Switches

by Catherine Redmond (catherine.redmond@analog.com)

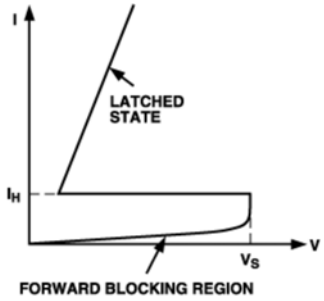
This article will briefly describe the causes, mechanism, and consequences of latchup and discuss available prevention methods. Although our aim is to give an understanding of latchup as it occurs in CMOS switches, similar principles apply to many other CMOS devices. *Latchup* may be defined as the creation of a low-impedance path between power supply rails as a result of triggering a parasitic device. In this condition, excessive current flow is possible, and a potentially destructive situation exists. After even a very short period of time in this condition, the device in which it occurs can be destroyed or weakened; and potential damage can occur to other components in the system. Latchup may be caused by a number of triggering factors, to be discussed below—including overvoltage spikes or transients, exceeding maximum ratings, and incorrect power sequencing.

CAUSE

For an understanding of latchup, it is desirable to briefly review the basics and understand the participating components. As already stated, latch-up occurs as a result of triggering a parasitic device—in effect an SCR (silicon controlled rectifier), a four-layer pnpn device formed by at least one pnp and at least one npn transistor connected as shown in Figure 1.



a) Transistor equivalent of an SCR.



b) Current- voltage characteristic of an SCR.

Figure 1.

An SCR is a normally *off* device in a "blocking state", in which negligible current flows. Its behavior is similar to that of a forward-biased diode, but conducts from anode, A, to cathode, K, only if a control signal is applied to the gate, G. In its normally off state, the SCR presents a high impedance path between supplies. When triggered into its conducting state as a result of excitation applied to the gate, the SCR is said to be "latched". It enters this state as a result of current from the gate injected into the base of Q2, which causes current flow in the base-emitter junction of Q1. Q1 turns on causing further current to be injected into base of Q2. This positive-feedback condition ensures that both transistors saturate; and the current flowing through each transistor ensures that the other remains in saturation.

When thus latched, and no longer dependent on the trigger source applied to the gate (G), a continual low-impedance path exists between anode and cathode. Since the triggering source does need not be constant, it could simply be a spike or a glitch; removing it will not turn off the SCR. As long as the current through the SCR is sufficiently large, it will remain in its latched state. If, however, the current can be reduced to a point where it falls below a holding-current value, I_H, the SCR switches off. Figure 1b shows the current-to-voltage transfer function for an SCR. In order to bring the device out of its conductive state, either the voltage applied across the SCR must be reduced to a value where each transistor turns off, or the current through the SCR must be reduced below its holding current.

A CMOS switch channel effectively consists of PMOS and NMOS devices connected in parallel; control signals to turn it off and on are applied via drivers. Since all these MOS devices are located close together on the die, it is possible that, with appropriate excitation, parasitic SCR devices may conduct — a form of behavior possible with any CMOS circuit. Figure 2 illustrates a simplified cross section showing two CMOS structures, one PMOS and one NMOS; these could be connected together as an inverter or as the switch channel. The parasitic transistors responsible for latch-up behavior, Q1 (vertical PNP) and Q2 (lateral NPN) are also shown.

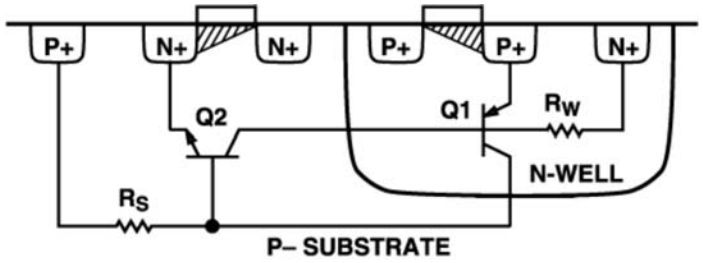


Figure 2. Cross-section of PMOS and NMOS devices, showing parasitic transistors Q1 and Q2.

P- substrate is used in devices from the ADG7xx family of switches and multiplexers, while devices from ADG4xx and ADG5xx families use N+ substrate. From Figure 2, it can be seen that a reinterpretation of the silicon configuration shows that the inherent parasitic bipolar transistors, Q1 & Q2, produce the parasitic SCR structure discussed above (Figure 3).

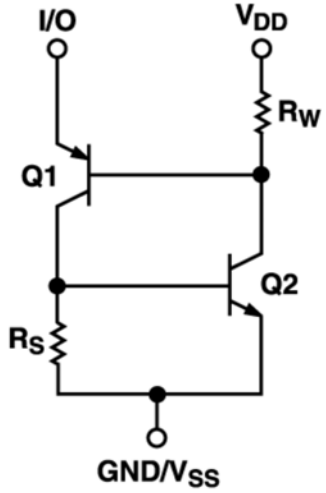


Figure 3. Rearrangement of the way we view the parasitic bipolars of Figure 2 shows an SCR structure.

Triggering mechanisms

Having described the architecture that makes latchup possible, we now discuss the events that can trigger such behavior. SCR latchup can occur through one of the following mechanisms.

- *Supply voltages exceeding the absolute maximum ratings.* These ratings in the data sheet are an indication of the maximum voltage that can safely be applied to the switch. Anything in excess may result in breakdown of an internal junction and hence damage to the device. In addition, operation of the switch under conditions close to the maximum ratings may degrade long-term reliability. It is important to note that these ratings apply at all times, including when the switch is being powered on and off. The triggering mode could result from transients on supply rails.
- *Input/output pin voltage exceeding either supply rail by more than a diode drop.* This could occur as a result of a fault on a channel or input—if a part of the system is powered on prior to the supplies being present at the switch (or similar CMOS components in the system). The powered part of the circuit would be sending signals to other devices in the design which may not be able to handle the voltage levels presented. The resulting voltage levels could exceed the maximum rating of the device, and possibly result in latchup. Again, this could occur as a result of spikes or glitches on input or output channels.
- *Poorly managed multiple power supplies.* Switches that have multiple power supplies tend to be more susceptible to latchup resulting from improper power-supply sequencing. Such switches usually have two analog supplies, V_{DD} and V_{SS}, and a digital supply, V_L. In some cases, when the digital supply is applied prior to the other supplies, it may be possible for maximum ratings to be exceeded and the device to enter a latchup state. In general, for those devices that require an external digital supply, V_L, we recommend that when power is being applied to and removed from the device, care should be taken to ensure the maximum ratings are not exceeded.

When any of the triggering mechanism described above occur, the parasitic SCR structure of Figure 1a may begin to conduct, producing a low impedance state between power supply rails. If there is no current limit mechanism on the supplies, excessive current will flow through this SCR structure and through the switch. This could destroy the switch and other components if allowed to persist. With high current levels, a device would not have to remain in a latch-up state for very long; even very brief latchup can result in permanent damage if current is not limited.

Protection and prevention

But such a fate is not inevitable in CMOS circuitry. The simplest way of preventing latch-up occurring is to adhere to the absolute maximum ratings. But if this is not always possible, there are other methods of designing a latch-up-proof system.

Here are some options for protecting against and preventing latchup: Where it is possible for digital or analog inputs to exceed the V_{DD} supply—either while power is being applied or during operation—the addition of a diode connected in series with V_{DD} prevents base current from flowing, thus avoiding SCR triggering and hence latchup. While Figure 4 shows the case where the *digital* input is exceeding the supply of the switch, IC#2, the diode also protects against overvoltages applied to the switch's *analog* signal path.

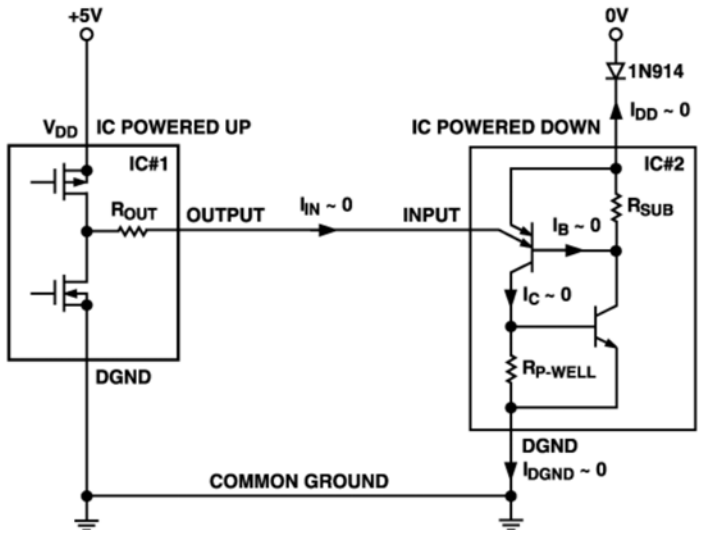


Figure 4. Addition of a diode in series with V_{DD} prevents SCR triggering.

Now, consider a switch with multiple supplies, where for example, the digital supply, V_L, may be applied to the device prior to other supplies, exceeding the maximum ratings and exposing the circuit to the potential for latch-up. Internal ESD (electrostatic-discharge-limiting) diodes may get turned on, so the simple addition of a Schottky diode, connected between V_L and V_{DD} (Figure 5) will adequately prevent SCR conduction and subsequent latch-up. This works very well; it ensures that when V_L and V_{DD} are applied to the switch, V_{DD} is always within a diode drop (0.3 V for Schottky) of V_L, so the maximum ratings are not exceeded.

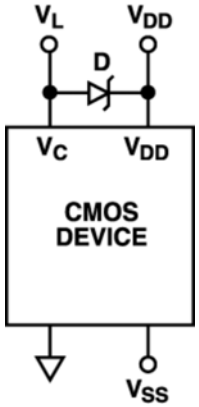


Figure 5. Addition of a Schottky diode from V_L to V_{DD} ensures max ratings are not exceeded.

Where the addition of an extra component is not a viable option, due to cost or limited board space, switches are available that have been manufactured on a process ensuring they are latch-up proof. The process uses an insulating oxide layer (trench) between the NMOS and PMOS devices of each switch. This oxide layer is both horizontal and vertical, producing complete isolation between MOS devices as shown in Figure 6.

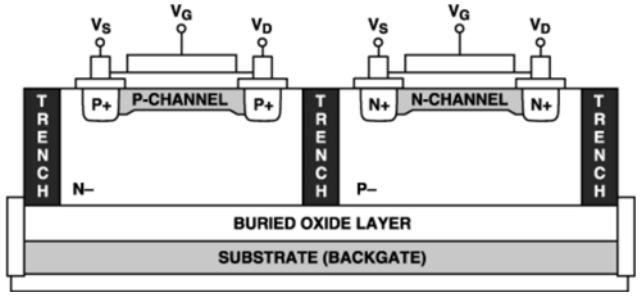


Figure 6. Cross-section of switch manufactured with trench processing.

This eliminates the parasitic bipolar devices between transistors, resulting in a latch-up proof switch. "Latchup-proof" means that no matter what way the power is sequenced to the device, latchup cannot occur.

Table 1 lists Analog Devices switches, multiplexers and channel protectors that have such processing. [For more information on Analog Devices switch products (including high-speed crosspoint switches), click here.] Although all the devices listed are latchup proof, not all are designed to handle *overvoltages* outside the supply rails, as the table indicates. In addition to these latchup proof switches, there are other devices that can tolerate under- and overvoltages, with power applied, of +40 V/–-5 V in excess of supplies and +55 V/–40 V with power not applied to the device. These devices are specifically designed to ensure that they can handle faults in the event of power-on or -off conditions. They also employ the insulating oxide layer to protect against latchup. They are available for use as either multiplexers or as *channel protectors.*

Table 1. Latchup proof Analog Devices switches, multiplexers and channel protectors.

Part Number	Function	Latchup Proof	Over/Under-voltage Capability	Package[1]
ADG431A	Quad SPST (NC)	YES	NO	R-16
ADG432A	Quad SPST (NO)	YES	NO	R-16
ADG433A	Quad SPST (2NC, 2NO)	YES	NO	R-16
ADG441	Quad SPST (NC)	YES	NO	R-16, N-16
ADG442	Quad SPST (NO)	YES	NO	R-16, N-16

ADG444	Quad SPST (2NC, 2NO)	YES	NO	R-16, N-16
ADG511A	Quad SPST (±5 V, 5 V, 3 V)	YES	NO	R-16
ADG512A	Quad SPST (±5 V, 5 V, 3 V)	YES	NO	R-16
ADG513A	Quad SPST (±5 V, 5 V, 3 V)	YES	NO	R-16
ADG438F	Octal 8-1 Channel Multiplexer	YES	YES	R-16, N-16
ADG508F	Octal 8-1 Channel Multiplexer	YES	YES	RN-16, RW-16, N-16
ADG439F	Differential 4-1 Channel Mux	YES	YES	R-16, N-16
ADG509F	Differential 4-1 Channel Mux	YES	YES	RN-16, RW-16, N-16
ADG465	Single Channel Protector	YES	YES	RT-6, RM-8
ADG466	Triple Channel Protector	YES	YES	RM-8, R-8, N-8
ADG467	Octal Channel Protector	YES	YES	RS-20, R-18

1 N = DIP, R/RN = 0.15" SOIC, RW = 0.3" SOIC, RS = SSOP, RM=microSOIC, RT = SOT-23

The multiplexers use a structure having n-channel, p-channel, and n-channel MOSFETs in series (Figure 7) to provide both device- and signal-source protection in the event of an overvoltage or power loss. The multiplexer can withstand continuous overvoltage inputs from –40 V to +55 V. When one of the analog inputs or outputs exceeds the power supplies, one of its MOSFETs will switch off, the multiplexer input (or output) appears as an open circuit, and the output is clamped to within the supply rail, thereby preventing the overvoltage from damaging any circuitry following the multiplexer. This protects the multiplexer, the circuitry it drives, and the sensors or signal sources which drive the multiplexer. Figure 7 shows what happens on one channel of the ADG438F in the event of a positive overvoltage. Because the fault protection works regardless of the presence of supplies, the muxes are also ideal for use in applications where power sequencing cannot always be guaranteed to protect analog inputs, (e.g., hot-insertion rack systems).

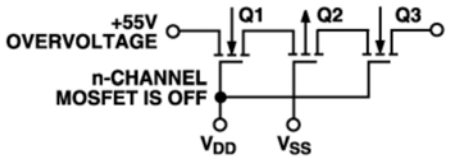


Figure 7. +55 V overvoltage applied to the input channel of ADG438F/ADG439F multiplexer in ON state.

Similarly, *channel protectors* are used to protect sensitive components from voltage transients in the signal path, whether or not the power supplies are present. They are built like the fault-protected muxes described above. When powered, the channel is always in the ON condition, but in the event of a fault, it clamps the output to within the supply rails, as shown in Figure 8.

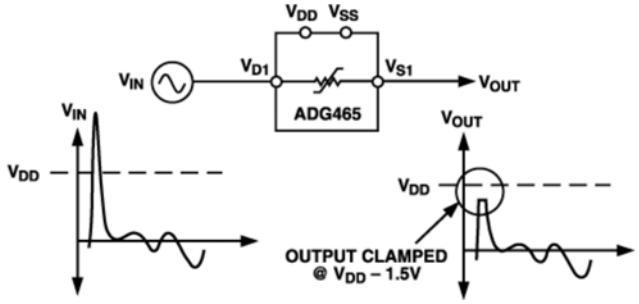


Figure 8. Channel protector clamps overvoltages to within power supply rail voltage and protects sensitive components.

Channel protectors are generally placed in series with the signal path ahead of standard CMOS-processed devices to ensure that potential faults can be tolerated without damage to components in the system. A common way of protecting a channel from potential faults, in either a powered or non-powered condition, is to connect diodes and current limiting resistors between the channel and the supplies. While it is an effective solution, it requires three extra components per channel, plus the board space to accommodate them. A channel protector would be an equally effective but simpler solution in a single small package.

For example, a channel protector could be used in conjunction with an ADC, switch, multiplexer or other device to ensure that all the channels are protected, both in the event of an over- or undervoltage, and a fault when the system is unpowered. These devices can withstand continuous voltage inputs from -40 V to +40 V. Because the channel protection works regardless of the presence of supplies, channel protectors are also ideal for use in applications where power sequencing cannot always be guaranteed to protect analog inputs, (a familiar example is hot-insertion rack systems).

CONCLUSION

Inasmuch as no application can tolerate latchup, it is necessary to be aware of its possibility, understand it, protect against it, and take measures to prevent it from happening. Given some thought and the use of available methods and components, it is indeed possible to assemble a latchup-proof system. While discrete solutions—such as diodes—could be used, devices like latchup proof switches, fault protected multiplexers and channel protectors may provide a simpler, more-compact, and more generally suitable solution, resulting in a robust system likely to give fewer problems in the field.