

## **SEUs and Their Effect on Electronic Devices Company: VideogeniX**

Single Event Upset (SEU) is one of the terms used by the computer and electronics industry to describe a phenomenon which causes electronic devices to lock up or become unstable. No matter which term is used - locking, latching, freezing – the end result is the same; a device that is no longer functioning in its normal operating manner. This natural phenomenon happens to every digital electronic device – including computers, cell phones, switches, routers, modems, gateways, PDAs, etc. Despite extensive research by universities, governments, and major fortune 100 companies no reasonable solution has been developed to protect commercial grade electronics from SEUs.

Many years of study have determined that SEUs occur in digital circuits when an energized particle, such as an electron, causes a transistor to change states from its correct state. This happens in microcircuits including: memory chips, communication devices, power circuits, microprocessors, etc. Such a flip of one bit can cause a computer or other electronic device to lockup, crash or become unstable.

### **What Causes an SEU?**

According to Altera<sup>1</sup> Corporation of San Jose, Calif., alpha particle radiation and atmospheric neutrons – which originate from the effects of cosmic rays – are the main cause of SEUs in semiconductor devices. Studies over the last 20 years have led to increased purity in semiconductor packaging materials, minimizing the effects caused by alpha particle radiation. This leaves unavoidable atmospheric neutrons as a primary cause for SEUs. SEUs were first observed between 1954 and 1957, when electric monitoring devices displayed anomalies during an above-ground nuclear testing. Further problems with SEUs – this time caused by neutrons from cosmic rays – were observed in space in 1975<sup>2</sup>.

### **Terrestrial SEUs**

SEUs don't just happen in deep space or when high levels of radiation are present. The same cosmic rays that warm the earth's atmosphere carry energetic particles that cause upsets in earth-based equipment. In 1979, James Ziegler of IBM and W.A. Lanford<sup>3</sup> first described how terrestrial cosmic rays could cause single event upsets (SEUs) in electronics. Over the next 15 years, IBM, led by Ziegler, continued to study SEUs, finding that while the rate of upset decreases as altitudes approach sea level, on average, every semiconductor device – such as an imager or memory cell in a digital camera – experiences an SEU approximately once a year. Because this is the average, it's reasonable to expect that some electronic devices may experience no upsets in a one year period while others may experience multiple. In addition to IBM, many other semiconductor companies including Motorola, Cray and Fujitsu have studied SEUs extensively. Their findings discovered additional causes of upsets here on Earth. These causes include power glitches, alpha particles, silicon impurities, software

---

1 Altera Corporation: "Single Event Upset," <http://www.altera.com/products/devices/stratix/features/stx-seu.html>

2 Normand, Eugene: "Single Event Upset at Ground Level," Boeing Defense &Space Group, Seattle, Washington.

3 Ziegler, J.F. and Lanford, W.A.: "Effect of Cosmic Rays on Computer Memories," Science, Vol. 206, pp. 776, 1979.

(<http://www.sciencemag.org/cgi/reprint/206/4420/776.pdf>)

bugs, and overall product quality issues. Additionally studies show that the number of upsets increases as the amount of transistors in these devices increase. Therefore, as memory capacities and transistor densities continue to increase, so will the number of SEUs in devices which employ them.

Today, we are more dependent on digital technology than ever before. Over the past several years, advances in digital technology have impacted our lives in almost every aspect – from cell phones to iPods, from PDAs to cameras. All of these devices today contain computers with microprocessors, software, memory, communication hardware – in other words, they are all susceptible to SEUs and other forms of lockup.

### **SEUs and the Security Industry**

Digital technology has also grown more prevalent in security industry products such as alarm panels, fire detection systems, access control systems, biometric security systems and digital security cameras. Of the more than 12 million security cameras that will be sold in the United States this year, more than 25 percent are expected to be digital and that percentage is expected to continue to grow each year. Considering only the SEU as a potential source of failure and that every one of these cameras has the potential to experience one, would result in approximately 3 million upsets on a yearly basis. This figure does not include all the digital cameras that are already installed. The impact of SEUs, power outages, software glitches, brownouts and other failure phenomena on the stability of security cameras or other mission critical devices is serious. When a camera locks up at a casino, the result is the immediate closing of a table or group of machines – and lost income for the casino. A camera lockup at an international border or nuclear plant could have more serious consequences. Based on a conservative average of one SEU per device per year, a 24-camera project, would experience an SEU-based failure about once every two weeks.

Each time a device locks up someone must disconnect the power, wait a few seconds and then reconnect the power. In many instances, customers claim this is the responsibility of the integrator. This results in a costly, time-consuming service call that often requires a ladder and possibly a bucket truck to reach the locked-up camera. Each service call results in diminishing customer satisfaction and an installer's diminishing return. If this happens every few weeks to every installed 20+ camera system, it's easy to recognize the drain on time, opportunity and resources SEUs alone cause. In spite of this evidence, many integrators are not providing customers with complete solutions to deal with lockups. Based on the decades of research by IBM, Motorola, Cray Computer, Altera, NASA and others who have studied the SEU phenomenon, we know that lockups are a fact-of-life. To combat non-SEU failures, a few manufacturers include a software watchdog in their digital cameras. In theory, the watchdog will restart the camera if there is a problem. However, a camera with a watchdog can't reset itself once the camera has locked up because in most instances the watchdog is part of the digital electronics itself, which is frozen.

There is no practical mechanism to prevent SEUs from occurring but everyone who's ever experienced an electronic device freezing knows that the solution is relatively straightforward: simply switch the device off, and then turn it back on. While this sounds easy, it could be prove to be extremely costly and time consuming depending on the location of the device.

## **How NASA Solved the Problem**

In 1999, NASA sent a complex digital camera into space as part of its Chandra X-Ray Observatory<sup>4</sup>. This space telescope relays images of the universe back to scientists here on Earth. These scientists are using the information gathered by Chandra to rewrite textbooks on the origin and evolution of the universe. Of course, a single SEU in Chandra's digital camera would have caused the entire project to be rendered useless – and the billions of dollars that went into Chandra would be wasted. From its prior experiences, NASA was already aware of the potential for SEUs, particularly in space, where alpha particle radiation and atmospheric neutron penetration are significantly higher. NASA worked with MIT to develop a mechanism that would monitor Chandra's electronics, including its digital camera, and, if necessary, reach across millions of miles and reset the camera automatically. This project cost millions to accomplish. As a result of the watchdog-like mechanism that NASA included in the project, Chandra has been going strong for more than seven years – well beyond its planned five-year mission.

## **A Solution for Earthbound Applications**

Glen Schaff, who had been the chief technology officer for VideogeniX, was a senior software engineer for NASA's Chandra project at the Massachusetts Institute of Technology's Center for Space Research. Having implemented the original space camera for Chandra, and recognizing similar security industry concerns regarding device failures, he and his partner, Eric Louis applied their joint expertise to develop a similar failsafe unit for digital IP cameras here on Earth. As a result, VideogeniX has developed iPulse®, a low cost solution that minimizes the potential effects of SEUs and all other natural upsets on electronic devices.

## **How iPulse® Works**

iPulse® measures 1 ¼" x 2" x ¾" but works in much the same way as the much costlier NASA mechanisms. Once an upset has been detected, iPulse starts a chain of events that automatically cuts power to the device, waits a few seconds, and then turns on the power – restoring the affected camera to working order. And because iPulse is separate from the device's internal electronics, it is not susceptible to the same fate as camera watchdogs in the event of an internal lockup. iPulse monitors the device's communication, and through its "patent pending" algorithms, recognizes when a lockup occurs. iPulse connects directly to the device's power source and sends power to the camera through a switchable cable – allowing it to continue to receive power while restarting the camera. In the event that the monitoring software fails or is not installed properly, VideogeniX has an optional automatic reset time frame built in as a fail-safe measure. At a pre-selected interval, iPulse can also perform an automatic restart every 12 hours, 24 hours, 2 weeks – or whatever time frame the user deems appropriate.

In the event of the unpreventable SEU, iPulse will have the device back up and running in less than a minute. If the device has a more serious problem, iPulse may also provide a signal that human intervention is required. iPulse is designed to support devices that run on

---

<sup>4</sup> National Aeronautics & Space Administration: "Chandra X-Ray Observatory," <http://chandra.nasa.gov>.

AC, DC and Power over Ethernet (POE). With multiple patents pending worldwide, iPulse is designed to work on virtually all wired or wireless digital network cameras, video servers and encoders. Since its introduction, iPulse has been successfully tested in the field on most major security camera manufacturers' products.

## **Beyond Cameras**

As all digital electronic devices are subject to lockup -- iPulse® was designed to accommodate all types of electronics and has been successfully deployed on many of them including: switches, routers, broadband Ethernet and cell modems, and access control devices. The possibilities and applications go far beyond cameras to the entire network electronics industry. In addition to iPulse being a standalone unit, the patent covers integration directly into other devices. Any device that might lockup can take advantage of iPulse® technology. So while no one can prevent SEUs from occurring, it's nice to know that iPulse provides a solution for minimizing the pain and keeping devices alive without human intervention.

For more information about iPulse, contact VideogeniX at 877-731-5550 or e-mail [info@videogenix.com](mailto:info@videogenix.com).