Military & Aerospace Electronics

December 2016

Technology Focus

Security and Solid-State Media Driving Data Storage

BY John Keller

It’s not enough to have rugged data storage with massive capacities and solid-state storage technology; today they also must offer multi-level data encryption, quick erase, and anti-tamper features.

The one-terabyte TRRUST-StorR SATA SLC self-encrypting solid-state drive (SSD) from Mercury Systems offers data protection and data management, protection from silent data corruption, and operational stability during power interruptions.

The rugged data storage business today is just as much about information security as it is about the actual storage media.

It’s a given that mission-critical aerospace and defense applications must store data on rugged and reliable disks and drives, yet today’s attention to cyber security also demands that data be reliably secure once it’s stored.

This confronts aerospace and defense electronics systems designers with a doubly difficult challenge for the future, because the military’s appetite for data never stops. Today we’re talking about rugged data storage systems able to hold terabytes of information, and a growing amount of it has to be secured.

In the recent past, systems designers used to talk about the need for megabytes and gigabytes of data storage capacity. Today we talk about terabytes, and soon petabytes, exabytes, and even zettabytes may enter the conversation. The continuing explosion of sensors, intelligence-gathering platforms, and real-time tactical networking all will keep the pressure on military data storage technologies.

Data storage media

Where years past saw a relatively even distribution in solid-state data storage and rotating magnetic media, the past two to five years have seen trends toward solid state. Today almost all aerospace and defense data storage for deployed applications have moved to solid-state memory.

"For us, we are focused on deployed applications, so it is really solid-state drives for us now," says Paul Davis, director of product management at the Curtiss-Wright Corp. Defense Solutions Division in Ashburn, Va.

"With solid-state costs coming down so much, we can get multi-level cell technology that supports wide temperature ranges," Davis says. "There hasn’t been applications where we can’t use them."

Although rotating magnetic storage media may have its niches, it’s largely disappearing in deployed military applications. "Most of our applications involve removable storage to take back to a ground station," Davis says. "You need to remove and carry those drives, and even the transport of rotating drives could get high levels of shock. Solid-state drives are more reliable."

It’s the same across many data storage applications for rugged deployed systems. "Everything we are involved in is solid state," says Ian Mackie, vice president and general manager of the Mercury Systems Microelectronics Secure Solutions business unit in Phoenix (formerly

White Electronic Designs Corp.). "Out in harsh environments where special security is a concern, I'm not aware of any rotating media anymore."

Rugged and reliable storage

Not only have the costs of solid-state data storage come down drastically over the past five years, but its reliability also has improved. "The technology is getting better and better," says Rodger Hosking, vice president at Pentek Inc. in Upper Saddle River, N.J. "A major benefit of the last five years has been solid-state drives are much faster and are suitable for high-vibration environments. They are smaller, lower weight, and the pricing is driven by commercial devices."

One knock against solid-state data storage in previous years was its endurance. Drives wore out in data-intensive applications if data transferred to data cells too many times. A lot of that has changed, Hosking points out. "There are more and more endurance cycles, and this is changing every few months."

Pentek and other companies that build and design-in solid-state storage are using a technology called wear leveling. This involves a data controller that keeps track of the number of times data writes to a solid-state drive's data cells. Then the controller distributes writes evenly to the drive's data cells so as not to use one memory cell too many times and wear it out.

Phoenix International's RPC24 high performance Fibre/SAS/iSCSI Host Channel, 6-gigabit SAS/SATA III solid-state/hard disk drive RAID subsystem offers self-encrypting drive (SED) technology, and support FIPS 140-2 certified AES 256 encryption as well as instant secure
erase.

The Pentek RTR 2623 6GHz RF Sentinel intelligent signal scanning portable, rugged recorder has an integrated 6GHz RF down converter for real-time signal monitoring and detection that is user configurable.

Amos Deacon III is president of longtime military data storage specialist Phoenix International in Orange, Calif. While Phoenix worked for years to ruggedize rotating magnetic disks for military and aerospace applications, much of the era of rotating media is coming to a close, Deacon acknowledges.

"Certainly it's heading in that direction; there's no doubt," Deacon says. "We have seen a significant increase in volume in our solidstate drives in the embedded space — particularly in the OpenVPX form factor, but also in our RAID disk array systems."

Although the cost of magnetic data storage still is far less than solid state, the price of solid-state storage has come down sufficiently to make it the more attractive option for aerospace and defense applications, Deacon says.

"I believe that the price point for SSDs has come to the point where it makes more sense for the users — for its performance and its environmental characteristics," Deacon explains. "For airborne

applications, almost everything we see these days is solid-state disk. The hard drive's big drawback is it needs an atmosphere to operate. Up above 10,000 feet, there is not enough air for the heads inside the hard drives not to crash against the disk of the storage media."

The big transition from rotating media to solid-state storage in aerospace and defense applications started about two years ago, and continues at an accelerating rate. "About two years ago, we started seeing a number of tech refreshes where we swapped-out rotating for solid-state disks," Deacon says. "What started people going in that direction was the overall reliability in those deployed environments."

In rugged conditions, there's just no beating solid-state storage these days, Deacon says. "In temperature extremes, altitude, and shock and vibration, it's much easier to create a system where you don't have to worry about cooling and shock isolation to the extent you did with a rotating hard drive," he says. "You still pay more for SSD, but you benefit on the back end because systems don't have to be so complex."

Data storage and data recording

Although a prime consideration in data storage is the sheer capacity of data-storage systems, a close second consideration is the speed at which a data-storage device can write and read data. Those systems designed reliably to read and write data in real time typically are called data recorder systems, rather than data storage.

"The difference between data storage and data recording is whether it is real time, or not," explains Pentek's Hosking. "With data recording you need to be doing it in real time. The whole key for what we do in recording is to guarantee we absolutely record data in real time, and never drop one bit of data that is being acquired. Eventually we will run out of total size, but that is a secondary concern to the rate at which we store data."

Data recorders typically are for intelligence-gathering systems that may have only one chance to capture crucial information on an adversary's radar system, new weapon, or military communications system.

Three things are key to a data recorder's speed. The first is how quickly analog information can be converted to digital data via analog-to-digital (A/D) converters. The second is the speed of a redundant array of independent disks (RAID) controller, and third is the speed of the data-storage medium itself.

"The price of solid-state storage has come down sufficiently to make it the more attractive option for aerospace and defense."

As far as the storage medium is concerned, solid-state is the choice for data recorders because it offers so much faster read and write speeds.

"SSD is much faster than the magnetic rotating drives we used 10 years ago," Hosking says. "We are constantly looking for the fastest data converters, the fastest RAID controllers, and the fastest storage media like solid-state drives."

A/D converters switch analog signals like radio waves into digital information. RAID controllers move digital data from A/D converters to the storage media. The storage media is where the data ends up. A delay in any of those three segments can spell the difference between real-time data recording, and non-real-time data storage.

Another technology advancement contributing to the speeds of data recorders are bridge chips that tightly couple PCI Express switches to multi-core microprocessors, Hosking says.

"That chipset provides an extremely high-speed path between PCI Express peripherals like data-acquisition boards and the RAID controller we are using for writing to the disks and to system memory," Hosking says. "We manage the interfaces on our boards from high-speed data converters through to PCI Express so we can write to system memory in real time."

With today’s data conversion and RAID controller technologies, data recorders can store data in real time at a bandwidth of about 1,500 MHz, says Pentek’s Hosking. "We can do a lot of what’s out there with what we have today," Hosking says. "Soon we will be able to double that with new products we are working on right now to get to 2.5 to 3 GHz signal bandwidth."

The Curtiss-Wright Data Transport System (DTS1) is a rugged network attached storage (NAS) file server for use in unmanned aerial vehicles (UAVs), unmanned underwater vehicles (UUVs), and intelligence, surveillance, and reconnaissance (ISR) aircraft.

There may come a time when technology advancements will blur the line between data recording and data storage. Phoenix's Deacon points to a new technology called Non-Volatile Memory Express (NVM Express). This eliminates the SATA or SAS interface and connects data storage directly to the PCI Express bus.

"In effect you're bypassing a network interface card, and the data storage connects directly to the CPU; it's extremely fast," Deacon says. "With NVM Express you're talking about 2,000 to 3,000 megabytes per second. It's a quantum leap in performance."

Security in data storage

With all the issues surrounding data storage for aerospace and defense applications, volume and speed of storage don't make up the whole picture. Data storage needs big volumes and fast speeds, but it needs security, too.

"Security is as important as anything else, and perhaps more important with regard to the nature of the data we are storing," says Mercury's Mackie. He's not the only such proponent. "In just about any new program

we work with now requires some level of data encryption," echoes Phoenix's Deacon. "If you're not able to support that, you're not a player."

The trend today is for evergrowing amounts of security in data storage. "I really see the trend heading toward more security," says Bob Lazaravich, director of research and development at the Mercury Systems Microelectronics Secure Solutions business unit in Phoenix. "Historically for cost reasons people have been using commercial drives not purpose-designed for this kind of application. That has been the trend, but in military applications we are considering military-level security, and unfortunately that's not free."

The chief concern of information security for data storage is preventing crucial data from falling into the wrong hands, whether the data drive has been lost, stolen, or captured. There essentially are three ways of doing that: encrypting the drive, erasing the drive, or sanitizing the drive. A fourth measure involves anti-tamper, which carries out one of the first three if sensors detect unauthorized attempts to access the data.

"I could envision a day coming when all military data storage will at least require encryption," says Curtiss-Wright's Davis.

Data encryption

The first way to keep stored data out of enemy hands is encryption. This involves using an encryption key to write and read data. There are several encryption schemes to secure military data, ranging from those administered by the National Institute of Standards and Technology (NIST), to higher levels of classification administered by the National Security Agency (NSA).

One good commercial level of encryption is FIPS 140-2, administered by NIST, which is common for military data drives. One readily accessible encryption method administered by the NSA is called Commercial Solutions for Classified (CSfC), which is a new way of delivering industry-developed and government-certified secure solutions quickly.

CSfC is based on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications. CSfC, however, falls short of the stringent levels of NSA Type 1 encryption, which must be provided by NSA-certified companies.

With encryption, the way to safeguard stored data from prying eyes is to destroy the encryption key. Although the data is still on the disk, it's virtually guaranteed that unauthorized attempts to access it will fail.

Crystal Group's RSS13S17 JBOD Rugged 1U Storage System, with up to six removable SATA/SAS hard drives and able to withstand the harshest environments, is designed for operational, deployable, and high-reliability applications.

The Model 9740 Complete Data Storage Solution from Kaman Precision Products' Memory Division is designed for use in severe environments, including military settings such as fighter aircraft, as well as other aerospace and industrial settings.

"The easiest approach is to blow away the key, so that nothing of the key is available in any part of the system," explains Mercury's Mackie. "So long as the key and its residuals are completely gone, we are assured that the data is completely safe as long as it's encrypted."

Although encryption might be fine for most data, those involving national secrets and national security require something more.

"We in our industry are paid to be paranoid, so we also would like to erase the whole drive," Mackie says. "We can erase a 1-terabyte solid-state drive in about four seconds."

The enabling technology for fast erase is NAND Flash solid-state memory, which is a type of non-volatile storage technology that does not require power to retain data.

Using the NAND erase command can wipe out data on all solid-state memory drive plans simultaneously. Some data storage designers use a command that erases the drive even if power is cut off mid-process. This command simply resumes erasing the drive when power is restored.

There even is a procedure that goes beyond erasing the data, called sanitizing, or zeroizing, the drive. This involves not only erasing the drive, but also over-writing the erased drive several times. The industry has four or five sanitizing algorithms, such as NSA 9-12, for data destruction, says Mercury's Mackie.

"Some drives we use have a signal — a circuit built in — that if you initiate sanitization it literally burns the circuits," says Phoenix's Deacon. "Once that starts, even if you pull power to that drive, as soon as you apply power again you can't stop it; it will continue."

There are times — particularly in forward-deployed military applications — in which security means the ability to erase or sanitize drives, and to do it quickly. This is another area where solid-state drives are superior to rotating media, because solid-state drives can sanitize in seconds, where rotating media might take hours.

"We are talking about where critical data must be protected from the enemy," says Mercury's Mackie. "If it is a warfighter's job to protect that data, we can do an erase in four seconds. Others might take tens of minutes to hours, and if a warfighter has to stay with the drive until it's erased, that's life or death."

"Even though you can sanitize it, if you can't sanitize it in the time frame the customer requires, you're out of the running," echoes Phoenix's Deacon.

The future of secure data

Experts agree that keeping data secure over time remains a moving target. Adversaries continually will find ways of defeating nearly every data security measure.

"You can imagine that attackers might use quantum computers to crack encryption," says Mercury's Lazaravich.

Quantum computers are different from binary digital electronic computers based on transistors, in that it uses analog signals and uses quantum bits, which can be in an infinite number of superpositions of states.

"The encryption we have today, while very good, won't last forever," Lazaravich says. "We'll need better encryption algorithms against the early quantum computers that will develop over the next five to ten years.

http://digital.militaryaerospace.com/militaryaerospace/201612?cmpid=navlink&pg=NaN#pgNaN