SiliconMotion

WHITE PAPER

How FerriSSD Ensures Availability, Longevity, and Security in Networking and Telecom

Ferri-SSD®

Telecom network operators, including 4G/5G and upcoming 6G mobile operators, are delivering more and more sophisticated services to ever-growing numbers of subscribers. These demands are changing requirements placed on networks. In addition to scaling to provide greater capacity and reach, they are increasing compute power in the edge to perform more intensive processing close to users, handle new workloads such as machine learning, and minimize latency.

Changes are happening throughout the network, all the way back to data centers and cloud servers that host large number-crunching applications and store vast quantities of data for retrieval and analysis.

On the other hand, while adapting to handle vast quantities of data quickly and efficiently, networks must meet additional critical requirements such as reliability, ruggedness, and security.

To meet these requirements, Silicon Motion has engineered high-performing and robust embedded storage solutions for cache and boot drives that meet the toughest expectations of network operators. This white paper assesses the attributes needed in a telecom-grade and embedded storage portfolio.

Challenges Facing Networking and Telecom Boot Drive

Telecom and Internet services sustain the fabric of modern work and life. Without connectivity, the critical services that keep businesses working (figure 1), research institutes learning, and transport networks running, and that support people with everything they need from online shopping and mobile banking to healthcare (figure 2), entertainment, and social contact would become unavailable.

Infrastructures are evolving to support a greater variety of more and more sophisticated services. Increasingly, these rely on cutting-edge computing techniques such as artificial intelligence and machine learning, leveraging algorithms hosted in the cloud as well as on platforms at the network edge. While the edge is undoubtedly becoming smarter, the cloud, also, is supporting more services, with more computing power, for more users, than ever before.

As greater intelligence spreads throughout today's networks, and the demands of professional and consumer end users continue to increase, infrastructure equipment is evolving to deliver higher performance, greater reliability, consistently high availability, and state-of-the-art cyber security.

Figure 1. Sample scene-setting image for business/industrial.

Figure 2. Sample scene-setting image for healthcare.

Embedded in the foundations of these networks, industrial-strength storage keeps user and program data safe and has a critical role in ensuring the availability end users expect with the durability and longevity operators need. It provides the key to consistent performance and must be robust, reliable, equipped to maximize data integrity, and capable of withstanding the hazards faced in harsh outdoor environments as well as resisting malicious cyber attacks.

Silicon Motion's Ferri embedded storage solutions are engineered to meet the diverse and stringent demands placed by today's telecom networks. Through built-in protection mechanisms, unique and

proprietary innovations to prolong lifetime and fine-tune performance, and cyber-security protection in accordance with the highest security-industry standards, the FerriSSD storage family is rugged and durable for deployment throughout today's rapidly changing networks.

Through their unique combination of industry-standard and proprietary and patented features they provide the expected attributes needed to keep today's networks functional and safe: end-to end data protection, extended cycle life, extreme environmental ruggedness, and high-grade security.

Superior Data Protection

Data integrity is a critical requirement and storage for telecom applications needs to take this to the highest level. SSDs for less demanding applications may implement error detection only at the front-end host interface and at the back-end NAND interface. This allows errors that can occur at other locations, such as internal SRAM and DRAM transfer buffers and other circuit paths, to go undetected. FerriSSDs contain full data-recovery engines to provide enhanced data integrity throughout the entire Host-to-NAND-to-Host data path (figure 3). The algorithms can effectively detect any error in the SSD data path, such as hardware errors, firmware errors and memory errors, including errors that are difficult to detect, such as soft error bits.

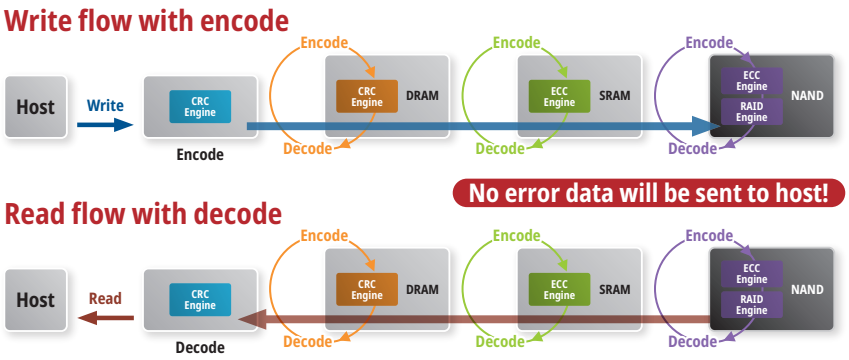

Figure 3. FerriSSD storage implements recovery engines for end-to-end data-path protection.

Also, in contrast with some conventional SSDs, FerriSSDs inform the host if any detected errors cannot be corrected thereby allowing the system to take appropriate action as necessary.

FerriSSDs deliver an additional advantage over conventional SSDs with extra features including the NANDXtend™ ECC Engine, as well as the proprietary IntelligentScan function and DataRefresh.

NANDXtend implements efficient second-level correction, above and beyond conventional first-level error correction that uses NAND shift-read-retries. It uses a low-density parity check (LDPC) code and a Group page RAID algorithm (figure 4) for redundant backup. Group page RAID minimises opportunities for uncorrectable errors and also extends the SSD service life.

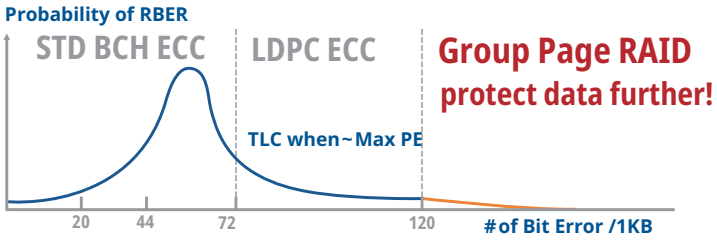

Figure 4. NANDXtend with special features like Group Page Raid significantly increases the cycle life beyond that of conventional NAND storage.

IntelligentScan and DataRefresh (figure 5) protect against data losses that can occur in conventional NAND flash as large numbers of program/erase (P/E) cycles are accumulated. Together, they automatically assess FerriSSD cell blocks and refresh or retire the blocks as needed to prevent these data losses. The scan frequency is automatically increased at higher ambient temperature to optimize data-loss prevention. A patented monitoring algorithm logs critical factors including cumulative junction temperature readings, the number of P/E cycles, SSD power-on time, and other essential reference points to dynamically select and prioritize NAND cells to DataRefresh.

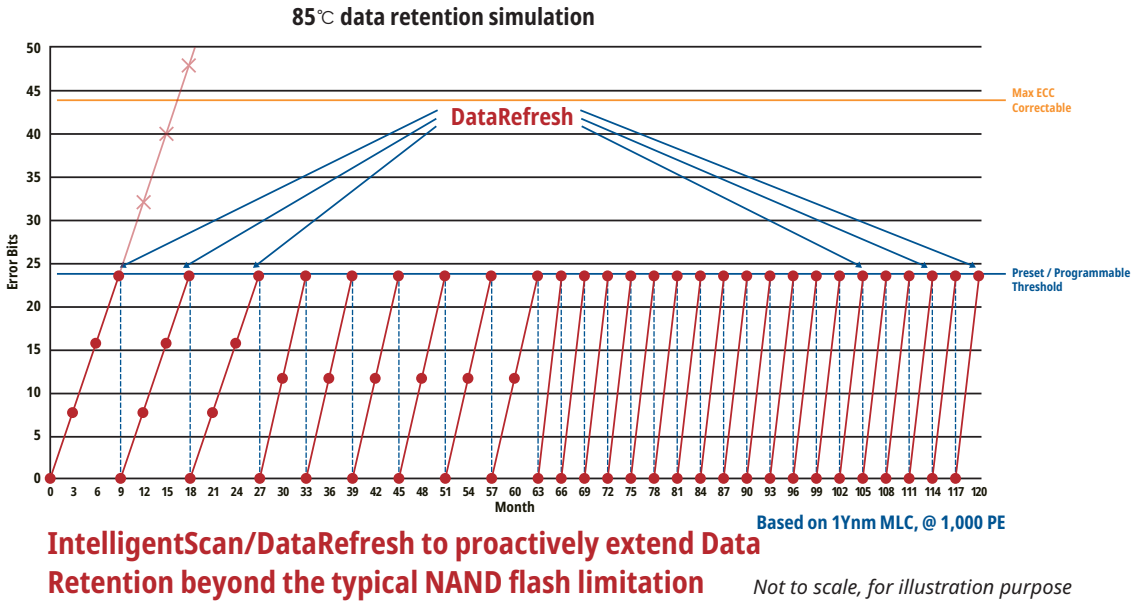

Figure 5. IntelligentScan and DataRefresh continuously monitor NAND cell contents to prevent data loss and correct errors.

IntelligentScan and DataRefresh also protect against data loss caused by read disturbances. Overall, their combined effect is to significantly extend the retention capability before data becomes unrecoverable, effectively prolonging the service life of FerriSSDs significantly beyond typical NAND specifications.

Sudden Power Loss Protection

Robust protection against unexpected power outages is always critical in telecom equipment. As well as backup power from a UPS, and ride-through circuitry inside power supplies and converters, data storage media need their own mechanisms to prevent data loss in the event of an outage. Sudden power loss protection in FerriSSDs triggers a data flush to safely store user data, taking power from an on-board back-up power supply.

Environmental Ruggedness

With the migration of intelligence into the network edge, smart infrastructure is deployed increasingly in outdoor environments that face hazards including extremes of temperature and humidity as well as environmental pollutants. In addition to dust and moisture, infrastructure equipment can be exposed to carbon particles as well as acidic and sulfurous compounds, particularly if installed close to highways (figure 6) or industrial areas where the environment can contain a high concentration of exhaust emissions and other chemicals.

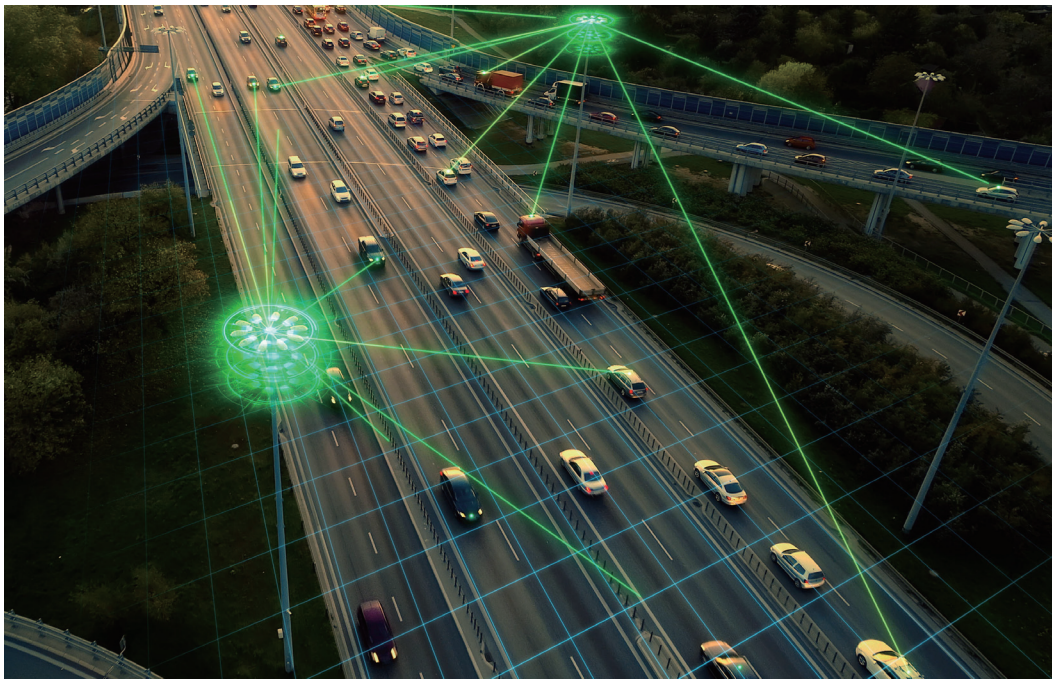

Figure 6. Sample image to illustrate outdoor deployment near highway.

FerriSSD modules are built using components that feature anti-sulfur terminal metallization to guard against corrosion and the module substrate is treated with conformal coating to ensure water and acid resistance. In addition, hard electroplated gold fingers maximize the durability of module-to-motherboard connections.

Each FerriSSD has a temperature sensor that allows, for instance, the host processor to slow read and write operations when a module is close to its maximum temperature threshold. This helps avoid the risk of damage or failure due to over-temperature.

In addition, FerriSSD's SMART SSD health log leverages built-in remote telemetry to enable operators to monitor the system and thus fully understand the SSD status. The telemetry data can help determine when to perform scheduled maintenance on devices and identify their location. Firmware upgrades can be applied, too, through this remote connection.

SSD security

Communication infrastructures face numerous cyber threats, ranging from opportunistic and nuisance hacking to organized cyber warfare that may have financial or strategic objectives.

It is vital that equipment can withstand such attacks, which typically aim to steal data and intercept or even disable communications. FerriSSD incorporates multiple protection mechanisms that leverage known industry best practice and state-of-the-art encryption. Together, these measures help protect privacy and intellectual property as well as to protect network operators against revenue losses and liabilities due to breaches and network outages.

Firmware Protection

To prevent attempts to take over or sabotage equipment, every FerriSSD storage device implements authenticated firmware protection. Known attacks include attempts to spoof the system by over-writing firmware with malicious code to be loaded when the system boots up and allow rogue agents to take control. They may try to force the disk to decrypt the stored content, expose sensitive data, or activate ransomware. The reference signature is stored in the FerriSSD using a built-in electronic fuse (eFuse) that is inaccessible from outside. If the firmware signature fails to match this reference, it will not be loaded and the system will not run. The secure digital signature also allows firmware updates to be applied remotely to FerriSSD units.

Spoofing emergency maintenance is another known form of attack. A FerriSSD will always send an alert to the host processor when it detects this type of activity.

Protecting User Data

To prevent unauthorized access to user data, FerriSSD products implement full disk encryption using industry-standard 256-bit AES cryptography. AES-256 cryptography takes millions of computing hours to crack by brute force and is trusted by government agencies, financial institutions and the military to protect sensitive data. The encryption is implemented in conformance with the latest Trusted Computing Group (TCG) standard, Opal 2.0, which helps ensure the drives are as secure as possible against unauthorized attempts to access the data stored on the disk.

In addition, the small size of FerriSSD products effectively discourages some kinds of physical attacks, such as probing and power analysis. FerriSSDs have up to 960GB storage capacity yet are delivered in a 16mm x 20mm surface-mount BGA package that can be mounted alongside the host processor inside the main enclosure of the device (table 1). This offers greater protection against physical tampering than a discrete, external SSD located separately from the motherboard.

All FerriSSDs support a Secured Quick Erase function, which can instantly delete all data if interference is detected. A hardware pin is also provided to trigger a data-flush sequence that safely stores user data during an unexpected event such as a sudden power failure.

Product series	PCIe FerriSSD	SATA FerriSSD
Package type	BGA	BGA
Host Interface	PCIe 3x2 (4) PCIe 4x2 (4)	SATA 6Gb/s SATA 3Gb/s
Dimensions	20×16mm	20×16mm
Capacity range	4～960*GB	4～960*GB
NAND type	SLCmode TLCmode	SLCmode TLCmode
DRAM	HMB support	Built in DRAM

Table 1: Ferri Embedded Storage Basic Specifications
*Mass production of PCIe 4.0 and 960GB is expected in Q1, 2023

Superior Product Quality Assurance

As a high-quality industrial-grade data-storage product, FerriSSDs are supported through consistent manufacturing and testing processes with associated documentation that attests to conformity. FerriSSDs always use the same part number as the qualified part. Each full part number means same fixed BOM (Build of Materials) and fixed firmware version. The consistent, high standard of traceability is applied to all materials used in each module and they are tested using an identical and consistent screening script.

Conclusion

Today's telecom infrastructures facilitate so many more activities in modern life than the telephone networks of past eras. The advanced digital services delivered, including messaging, social media, mapping and location services, streaming entertainments, and many more are regarded as essentials by users that demand easy access, fast response, and high availability. Network operators need to rely on extremely high system performance, ruggedness in indoor and outdoor environments, and resistance to cyber-attacks.

Silicon Motion's FerriSSD storage incorporates industry-standard and proprietary features to provide the qualities expected of infrastructure equipment: exemplary data integrity, resistance to harsh environments, extended cycle life, and resistance to unauthorized access and tampering. Through these means they are ready to fulfill boot drive applications in today's networking and telecom industries.

For more information about Ferri Family, please go to
www.siliconmotion.com or send email to **ferri@siliconmotion.com**