White Paper

Avoiding IoT Downtime and Cost Overruns with Secure Out-of-band Signaling

Executive Summary

This white paper outlines the use and advantages of out-of-band communication for Internet of Things devices enabled by solid-state drives with integrated Azure Sphere microcontrollers. It explains how this solution addresses the issues of IoT management, maintenance, and device security—ultimately providing a solution to reduce downtime and maintenance costs for IoT system operators.

Introduction

Boiling it down, the Internet of Things (IoT) is the concept of connecting existing devices and adding new devices to any network, be it internet or local networks. For companies aiming at increased digitization, IoT can be extremely beneficial in terms of streamlining operations and gathering data, often easing management and allowing for significant cost reductions.

As much as 80% of IT costs are incurred after the initial purchase, with downtime and maintenance ranking as the biggest sinners, according to Gartner.

What is often neglected are the associated complications caused by the increase of devices and relative reduction of human operators. Increased maintenance costs are bound to follow an increase in the number of devices, and so does the risk for downtime and inefficient management. According to Gartner, as much as 80% of IT costs are incurred after the initial purchase, with downtime and maintenance quoted as the biggest sinners.[1]

Fortunately, management systems can go a long way in mitigating these concerns. Ideally, the system provides the user with a good overview and enables remote backup and recovery, while also offering predictability. As a result, many companies have implemented such system health monitoring features and management routines into their products and software.

However, these features all rely on a risky assumption: that the device itself remains operational. In most instances when the operating system (OS) crashes, such management systems can no longer access the device. Consequentially, the only solution is to send a technician out to fix it manually—a costly and labor-intensive solution that is simply unsustainable in a world where the number of internet-connected devices is growing at an exponential pace.[2]

This white paper will explain how out-of-band storage solutions can overcome these challenges by leveraging an independent channel embedded in the solid-state drives (SSDs) of IoT devices.

Background

In-band and Out-of-band

Out-of-band is best explained by first looking at what in-band signaling is. In essence, in-band signaling basically covers all the typical ways we connect components and peripherals to a device. Using SSDs as an example, the in-band connection can be facilitated by the standard connectors you find on most motherboard like SATA, M.2, mPCIe, or even through USB and SD card ports. The in-band signaling to the device is dependent on the system, and, by extension, the OS, being up-and-running.

In contrast, out-of-band describes solutions with connections that circumvent the system to form an independent communication channel. With innovative edge solutions like the InnoAGE SSD, cutting-edge proprietary technologies allow the SSD to execute commands such as recovery, backup, and secure erase without depending on the rest of the system being functional. These technologies, combined with an advanced Wi-Fi transmitter-equipped MCU like the InnoAGE SSD's embedded Azure Sphere, makes it possible for the user to remotely access and control the SSD regardless of the overall system status.

Remote Management of Malfunctioning Devices

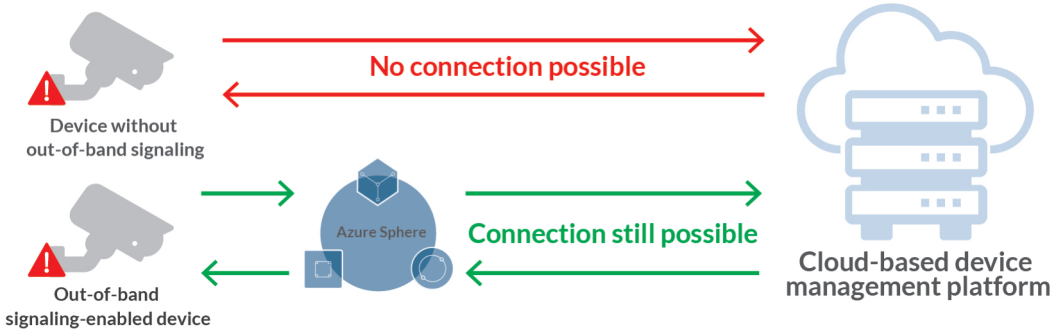

Image 1: Remote recovery available for the out-of-band signaling-enabled device through the Azure Sphere.

Azure Sphere

Azure Sphere is a Microsoft-designed MCU intended for use in IoT devices.[3] Functioning as a system in itself, the Azure Sphere runs the Azure Sphere OS, which allows the device to operate independently of the host device's OS. To ensure that the device remains fully protected against external threats such as unauthorized access attempts, Microsoft has created a powerful security suite to ensure device integrity and to protect the hardware from malicious actors. The security provided by the Azure Sphere also encompasses secure and encrypted access to Azure Cloud services.[4]

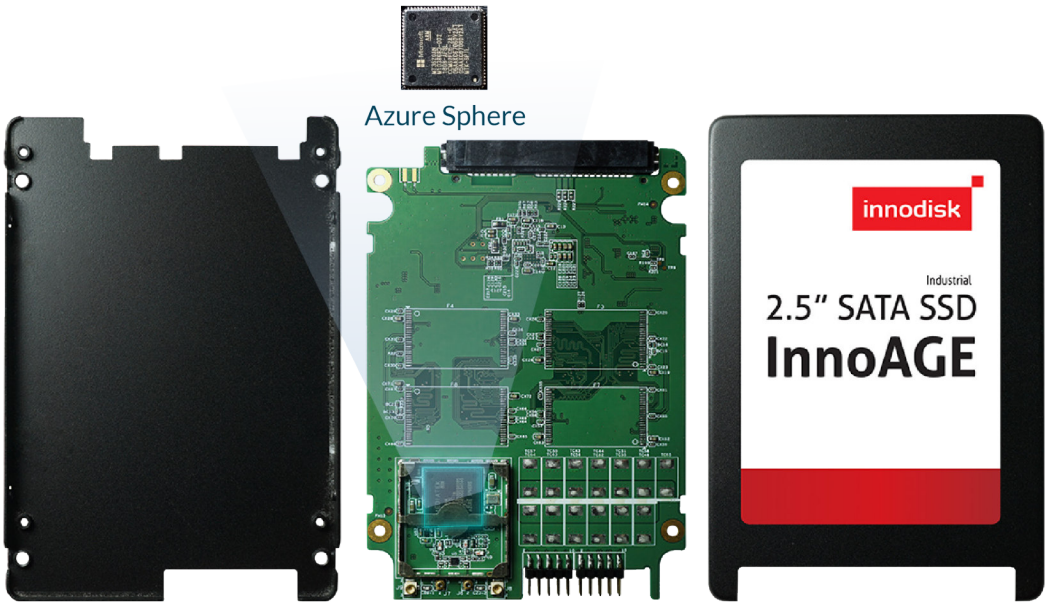

Image 2: Showing the InnoAGE SSD with an embedded Azure Sphere.

Challenges

The key challenges of a successful IoT expansion can be split into three main categories: management, maintenance, and edge security.

Management

The IoT management problem is two-fold. The first part is simply handling all your device data as it is being produced.[5] As the ratio between devices and device operators continues to grow, the difficulty of staying in full control of your system also increases. Without predictability, planning efficient management is close to impossible and leaves the system at risk of unexpected downtime.

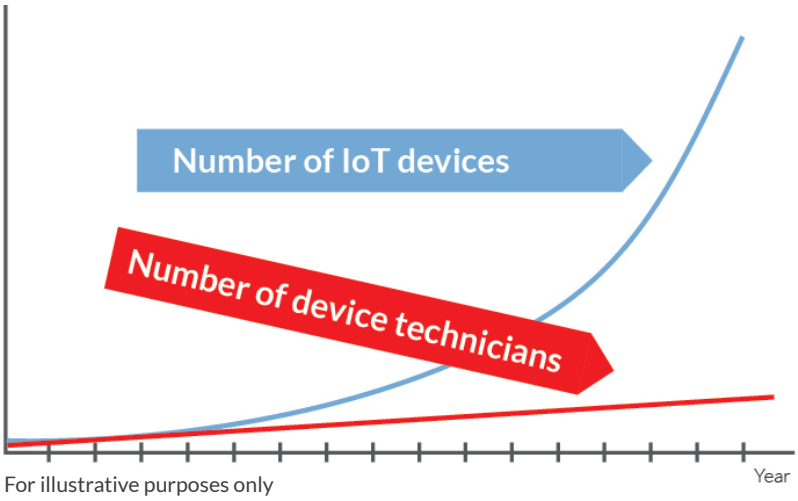

Image 3: The exponential growth of IoT devices leaves few technicians taking care of massive amounts of devices.

This brings us to the second part of the IoT management issue: in-band signaling dependence. To gather data from your IoT device, it has to be operational with the device OS running. This means that once the device fails or the OS crashes, the system integrator has to send someone to tend to the device. Most management systems available on the market today do not address this concern or only offer partial solutions to what remains a fundamental challenge in the race to a more internet-connected world.

Maintenance

Mismanaging maintenance will lead to significant costs incurred by the system integrator. For example, a vending machine that suddenly stops working will lose all business during the downtime. Additional costs are incurred by having to send someone to fix the issue that has occurred, and in the worst case, replacing the failed hardware.[6] At scale, for example a company that operates tens of thousands of vending machines, the aforementioned quickly turns prohibitively expensive.

The above underlines the fundamental requirements of efficient IoT maintenance: accessibility and speedy system recovery. The system needs to be readily accessible—even if the system itself crashes. It also needs to provide a certain level of predictability to prevent failures and allow efficient and timely maintenance. Lastly, once the system crashes, there need to be tools available to quickly fix and restore the system—preferably without needing boots on the ground.

Edge Security

Wide coverage of interconnected devices means more data and a more efficiently-run application. The downside is that with each device added to your network, there is one more potential entry point that can be exploited.

Since IoT devices are typically unmanned with limited physical operation and supervision, system integrators are required to address security risks faced by both the device itself and the networks that the device is connected to. This usually means multilateral solutions that address locally stored data as well as the device's communication channels.

When there is an integrated MCU involved, i.e., a device within the device, the edge security challenge is further compounded. If the MCU has a separate connection channel, this pathway must be secured in the same way as the device itself.

Solutions

Intuitive Management Platform

The first step in ensuring effective IoT management is gathering all connected devices on a single platform, such as Innodisk's iCAP™. The output from these devices then has to be presented in an easily accessible manner.

By having the output presented through a simple browser-based user interface, the information is easily accessible for all users, regardless of factors such as device and location. By establishing thresholds for pertinent parameters, for example temperature or the number of SSD write cycles, the management system also offers predictability, which in turn makes it easier to plan future work on the system's devices.

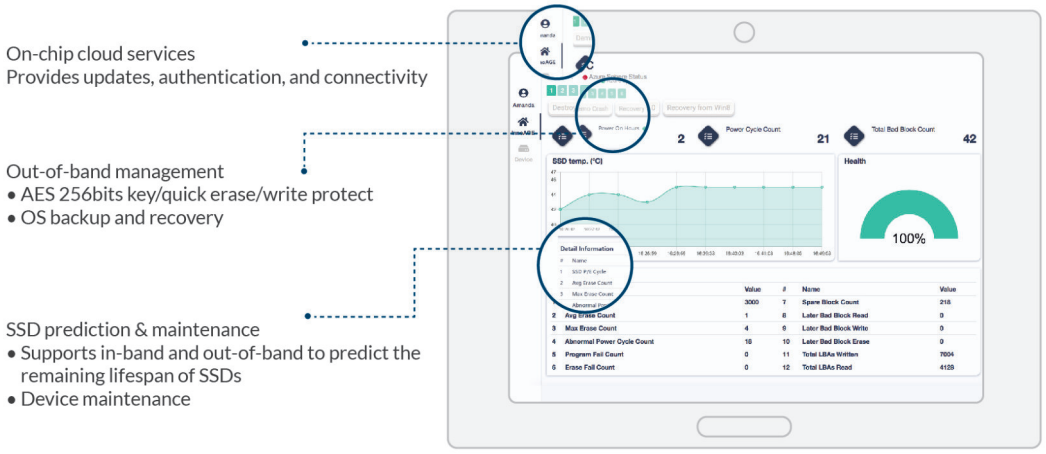

Image 4: Screenshot of InnoAGE SSD management platform.

However, these fundamental aspects of IoT management still leave the system vulnerable to sudden system crashes. Once the system is down, in-band management is impossible, rendering the entire management system useless pending a manual reset. This is why out-of-band signaling is a critical addition to any IoT management solution. By assuring constant access, the device is always ready for updates to its firmware, its embedded MCU, and other components.

There is one further avenue where in-band management can be strengthened: general purpose input/output (GPIO) customization. This refers to the customizable signal pins that are located on the circuit, for example in an SSD, whose behavior can be altered by the system integrator. This allows for additional security measures, such as secure erasure and data destruction.

Remote Maintenance Through In-band and Out-of-band Signaling

It is the goal of any system integrator to keep maintenance to a minimum while assuring maximum operability. Maintenance planning should also include planning for unforeseen crashes.

What this means is that any IoT system should have robust measures ready to handle sudden loss of device functionality. As an example, we have three factories with devices connected to a central cloud service via installed out-of-band SSDs (see image 5). With in-band signaling only, sudden device malfunction would only prompt a notification that the device stopped sending data. An operator would have to physically access the device to run tests and fix the problem.

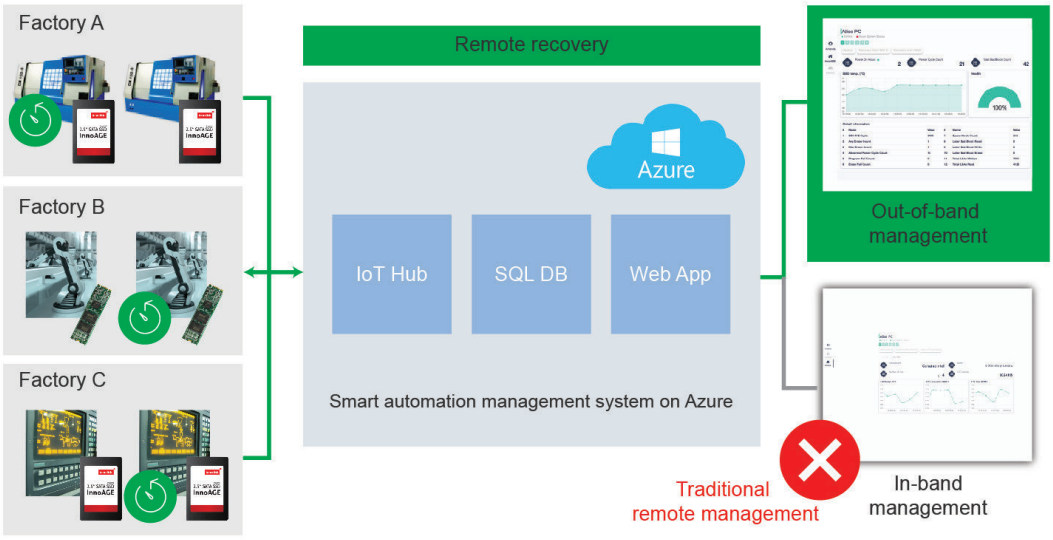

Image 5: Example of remote recovery through out-of-band management.

With an out-of-band solution, you can access the device and run diagnostics remotely. Furthermore, all out-of-band SSDs have one drive partition dedicated to recovery, meaning that a recovery image for the device OS is available at all times (see image 6).

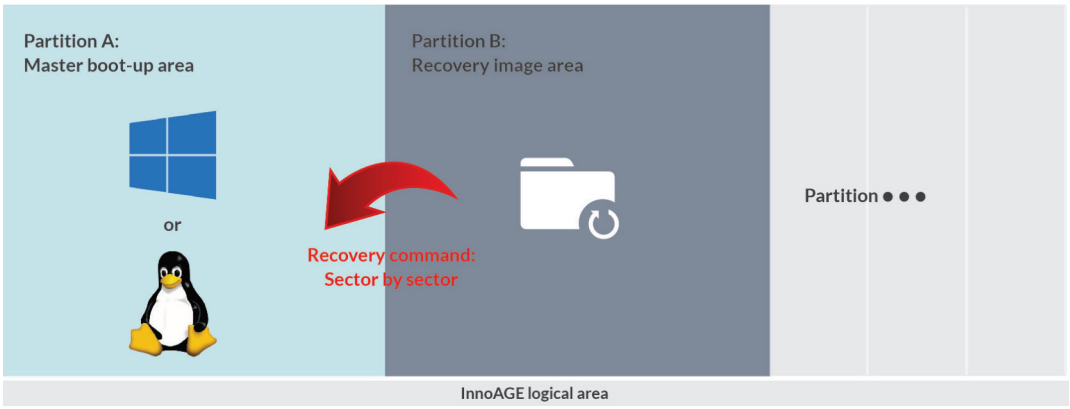

Image 6: An SSD partitioned for future recovery purposes.

MCU and Storage Device Security

Storage devices with out-of-band signaling are required to address data security on two fronts: local data and cloud data transmissions.

With locally stored data, there are several options to ensure data security. For example, AES encryption is possible with an integrated AES engine in devices such as the Innodisk InnoAGE SSD. This ensures that data going into the NAND flash is all encrypted with an inaccessible key. With an added security management system added on top, it is easy to set up a user system with different clearance and access levels.

For mission-critical applications, there are also options for secure data erasure and data destruction. This can be triggered remotely though both in-band and out-of-band channels to rapidly remove or destroy data that are in danger of being compromised.

The second layer is cloud transmission security. With the Microsoft Azure Sphere, this includes a multi-faceted security system to ensure that data between the cloud services and the MCU is rigidly protected.

Adding It All Together

For IoT system operators, adding all of the above together means a powerful toolset to take on IoT's biggest challenges. By making maintenance available on an intuitive management platform through both in-band and out-of-band signaling, the IoT system becomes vastly more scalable and significantly easier to maintain.

Thanks to fortified security both locally and in cloud transmissions, this can all be achieved without compromising system integrity.

Conclusion

SSDs with state-of-the-art software and embedded MCUs such as Innodisk's Azure Sphere-equipped InnoAGE SSD provide system integrators with an effective way to mitigate some of IoT's biggest challenges. By enabling out-of-band signaling, management and maintenance can be greatly facilitated while maintaining edge security at the highest level. The result is a solution that enables the future of an ever-growing number of connected devices while also reducing costs for IoT system operators.

For IoT system operators wishing to build connected systems that are sustainable in the long-run, out-of-band-enabled solutions are essentially a requirement.

References

1. https://www.gartner.com/imagesrv/media-products/pdf/XSI/1-5YQUH4Q/XSi_Third_Party_Maintenance.pdf
2. https://blogs.cisco.com/datacenter/internet-of-things-iot-data-continues-to-explode-exponentially-who-is-using-that-data-and-how
3, https://azure.microsoft.com/en-us/services/azure-sphere/
4. https://docs.microsoft.com/en-us/azure-sphere/product-overview/what-is-azure-sphere
5. https://www.ey.com/Publication/vwLUAssets/EY_-_Future_of_IoT/$FILE/EY-future-of-Iot.pdf
6. https://www.zinier.com/2019/03/20/three-ways-the-iot-is-changing-field-service/

Innodisk Corporation

5F., No. 237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Tel : +886-2-7703-3000
Fax : +886-2-7703-3555
E-Mail : sales@innodisk.com
Website : www.innodisk.com