hyperstone®

An Introduction to:

Industrial Gateways for 5G Networks

Choosing Storage for Ultra Reliable Systems

This white paper discusses the challenges faced while designing an industrial gateway connected by a 5G wireless network in regard to NAND flash storage.

www.hyperstone.com

Authors

The Hyperstone Team

1st. Edition

Table of contents

List of Abbreviations

4G	–	4th Generation of Mobile Communications
5G	–	5th Generation of Mobile Communications
5G-ACIA	–	5G Alliance for Connected Industries and Automation
CapEx	–	Capital Expenditure
CSP	–	Communications Service Providers
GB	–	Gigabyte
Gbps	–	Gigabits per second
IIoT	–	Industrial Internet of Things
IoT	–	Internet of Things
kB	–	Kilobyte
LTE	–	Long-Term Evolution
M2M	–	Machine-to-Machine
MB	–	Megabyte
MLC	–	Multi-Level Cell
NMOS	–	N-Type Metal-Oxide-Semiconductor
NVM	–	Non-Volatile Memory
NPN	–	Non-Public Network
NR	–	5G New Radio
OS	–	Operating System
P/E	–	Program/Erase
PCB	–	Printed Circuit Board
pSLC	–	pseudo Single-Level Cell
QLC	–	Quad-Level Cell
RAN	–	Radio Access Network
SLC	–	Single-Level Cell
SLS	–	Service Level Specification
TLC	–	Triple-Level Cell

1 Abstract

Continued adoption of connected devices across the globe is demanding faster data transmission rates from wireless networks due to the growth of mobile data traffic.

According to Gartner, in 2020, Communications Service Providers (CSPs) are predicted to have invested $38B globally. The Capital Expenditure (CapEx) on 5G reached $8B, showing close to a 100% increase in investment in 2020, compared to the previous year.

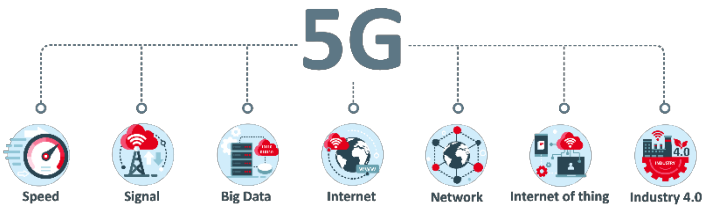

Figure 1 5G Networks, Key Themes

Gartner also expects that by 2023, 15% of CSPs worldwide will be operating stand-alone 5G networks, which means they will not rely on the current 4G/LTE infrastructure. Therefore, future investments are expected to be focused on 5G New Radio (NR) rather than legacy Radio Access Network (RAN) infrastructure.

This will enable new applications that make use of the key features and enhanced capabilities of 5G networks, such as

higher data rates, better synchronicity, higher reliability, and ultra-low latency.

By 2023, there is expected to be 4.4 billion M2M connections. This covers a wide variety of applications, from navigation systems in vehicles, asset tracking systems in logistics and predictive maintenance in manufacturing facilities, to medical applications that monitor vital statistics or make patient records more readily available.

New applications in the industrial segment are dependent on these new capabilities to maximize their value proposition, and as the potential unfolds, new ideas and use cases will follow.

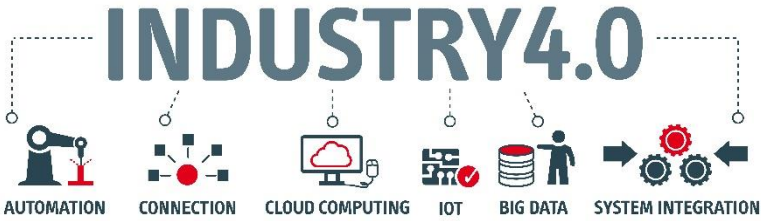

Figure 2 – Industry 4.0, Key Themes

This has led to a new ecosystem in the industrial market, interchangeably referred to as Connected Industries, Industry 4.0 and the Industrial Internet of Things (IIoT).

This paper exemplifies how the ability of industries to communicate with higher level applications, either locally or in the cloud, is changing commerce.

For the sake of this paper, the term “connected industries” will be used in reference to any production or manufacturing processes that demands the ability to communicate with other service platforms, over 5G networks or other technologies offered by CSPs.

This paper highlights the main demands that the connected industry makes on industrial storage, as it is applied to industrial IoT gateways. It covers the requirements that need to be met when connecting to 5G networks, both standalone Non-Public Networks (NPNs) and shared networks.

2 Introduction

Due to the large variety of communication technologies currently used in factories today, gateways have been introduced to connect existing and legacy devices to the new 5G infrastructure.

These gateways are essentially private 5G microcells designed to operate as part of the 5G network and provide a way to connect IoT devices which may be using multiple different protocols. As such, the gateway will need to function like a cellular base station. The code base for such a gateway will be comprised of an operating system, network layers and the protocols needed to interface to legacy devices. This will run to many millions of lines of code and require tens of gigabytes of persistent storage. This storage requirement can only be met using NAND flash, which comes with system-level requirements of its own.

As the rate of replacement in many industries can be measured in decades, the need for gateways is expected to remain for many years to come. If the data communication services delivered over 5G networks are to meet the Service Level Specification (SLS), these gateways must not impact performance. This means the gateway must match or exceed the cellular network's capabilities, while also meeting the requirements of connected industries, as listed below.

Network requirements for connected industries:

✓ Data rate	➲ several Gbps
✓ Synchronicity	➲ 1µs
✓ End-to-end latency	➲ ≈ 1ms
✓ Communication service availability	➲ > 99,999%
✓ Security	

Source: 5G-ACIA Web Seminar "5G Alliance for Connected Industries and Automation"

Maintaining this level of service makes every functional block in the gateway critical, including the wireless interface, the power supply, and the non-volatile storage. Considering the above requirements, it is important to have a solid understanding of what makes an IoT Gateway for 5G Networks industrial.

3 Gateways Connected to a 5G NPN

Industrial gateways are network-attached devices that can aggregate the many different protocols used by connected devices in a factory environment. In addition to operating as a cellular base station, they translate the various communication protocols used by other connected devices (sensors, actuators, and automated equipment). They encapsulate the data into a format which is suitable for transmission over a 5G radio interface.

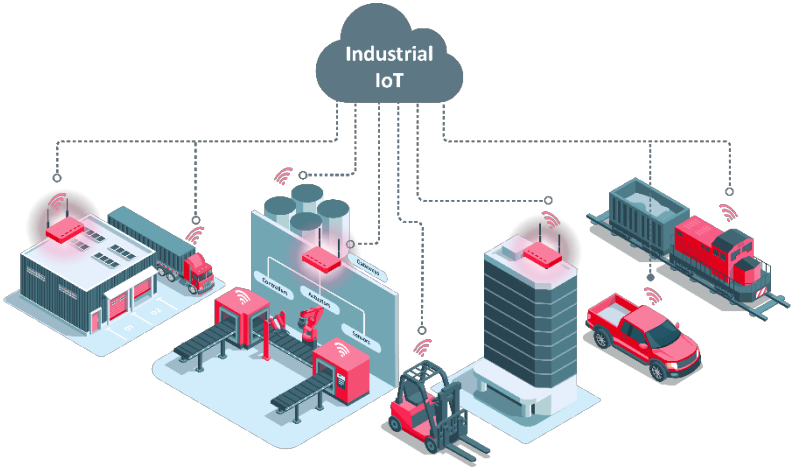

Figure 3 – Industrial IoT Network Infrastructure

As depicted in the above figure, the gateway has become an integral part of the 5G network. Since the SLS performance is heavily dependent on the gateway, it is necessary that its design

meets the same mission profiles of the 5G network. To ensure this happens, aspects such as reliability and security need to be carefully considered, in addition to the selection of the data storage embedded in any device.

4 Reliable Electronic Systems

All elements of an electronic system, including the electronic and electro-mechanical components and the PCBs, must meet the same design targets to support reliability, operating lifetime and the planned obsolescence of the system.

In the case of semiconductor design, rules are used to define physical features such as channel sizes, clearances and the interconnects that are needed to instantiate the cell structures, metal layers and many other geometric features. There will be tolerances associated with these features which are defined by the design rules. Through these design rules, the overall tolerances can be assessed, thereby enabling the manufacturer to specify the operating lifetime.

For example, a semiconductor specified for use in consumer products may be expected to be active for six hours per day, five days per week for a lifetime of five years, operating mainly at room temperature. This component would be designed differently than an industrial-grade component which has been specified to operate 24 hours a day, seven days a week for a minimum of ten years, in an outdoor environment.

The important design considerations extend to the smallest feature. For example, the leakage current of an NMOS transistor typically increases tenfold as the ambient temperature increases from 50°C to 100°C. Even the most efficient system will dissipate heat, causing the ambient to increase. In turn, this will increase the leakage current, generating even more heat

being, creating a positive feedback-loop. Considering that a higher operating temperature has a significant and negative impact on the operating lifetime of an integrated device, it is just one of the key parameters that need to be considered in the design of a semiconductor product to avoid unexpected field failures.

For NAND flash technology, high temperature and temperature variation will stress the cell at a silicon and system level, causing higher error rates which reduces overall storage and system lifetime. Specifying storage that features a flash controller which is optimized for a system's mission profile is extremely important in achieving a defined lifetime.

By the same logic, development of the software architecture should also follow the mission profile, paying close attention to reliability, in accordance with the component selection and guide-lining.

Finally, the manufacturing of the system and its subsystems should be considered. Aspects such as certification, quality, long-term supply management strategy, and security layers are also very important and should be addressed during the design phase to ensure the reliability of the product.

5 Selecting Reliable Storage

Selecting the right NAND flash, controller, and firmware will ensure that the intrinsic physical properties of the memory technology and its inherent weaknesses are properly managed. This allows the storage to meet its mission profile reliably.

Some of these mechanisms and effects that are relevant to reaching a superior storage system in endurance and extended lifetime are:

- Garbage collection and wear level management
- Write amplification, NAND flash lifetime
- Data retention and error correction performance
- Power consumption, and thermal management
- P/E cycles depending on SLC, MLC, and TLC NAND technology types
- Support of high-reliable NAND flash (e.g. SLC, pSLC)

Another important aspect of the design is security.

Due to the architectural evolution of microcontrollers, formerly on-chip embedded non-volatile memory, has gradually been replaced by external non-volatile memory chips and memory modules - typically based on NAND flash.

This evolved architecture exposes the physical interfaces between controllers and external memory devices, offering potential attack vectors for hackers and increasing the

vulnerability. Thus, connected systems become more susceptible to hacker attacks than non-connected systems.

As these systems become more intelligent and capable, they are taking on more critical activities like asset management, autonomous driving, and tasks such as medical assistance. The prevention of security breaches has become the highest priority within the engineering community.

The industry's response has been to develop a secure boot design, i.e., making sure the controller and the storage device can establish a secure Root of Trust during the boot-up stage.

The host controller must be able to verify that the code in the non-volatile storage that it accesses is original (signed) and has not been changed or tampered with. Or, if it has been changed, it must confirm that this was an authorized and verified update.

Ensuring a secure boot concept is a fundamental foundation of designing secure electronic systems.

The introduction of 5G gateways into industrial IoT environments will highlight the need for secure boot and the ability to establish a Root of Trust, which will influence the memory subsystem design choices made at a system level.

If you want to know more about NAND flash technology, please visit our website. We have a vast collection of white papers for

both beginners and advanced readers on the topic. Below is our recommended literature for beginners:

- Introduction to Non-Volatile Memory
- Introduction to Flash Controller Technology
- Introduction to Flash Memory Form Factors
- Introduction to Hyperstone Controller Technology

Key Take-Away: *Endurance, lifetime, and security create a reliable storage*

6 Conclusion

For an Industrial IoT 5G Gateway to meet all necessary aspects of the industrial-grade application, it is imperative that the right storage technology, vendor, and supply chain are selected.

For security, the origin of manufacturing and firmware provision should also be considered to ensure a secure Root of Trust mechanism between controller and non-volatile memory where boot code is stored.

When defining the architecture of such gateways, storage and security mission profiles are required to be as identical as possible to their 5G network mission profiles, ensuring the system solution can meet its end-to-end Service Level Specification.

It is critical to understanding the entire system's mission profile and confirm that the selected storage system (including NAND flashes used) meets all requirements imposed by a telecom-like equipment.

With extensive experience in delivering high-performance, secure, and reliable storage solutions, Hyperstone is ready to discuss any aspects of secure boot and non-volatile storage as they relate to creating an industrial gateway.

hyperstone®