TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MATTI FLOMAN

SOLID STATE MASS MEMORIES IN THE WORLD OF INTERNET OF THINGS

MASTER OF SCIENCE THESIS

Examiner: Professor Hannu-Matti Järvinen

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Information Technology
Floman, Matti: Solid state mass memories in the world of Internet of Things
Master of Science Thesis, 53 pages, 1 Appendix page
August 2015
Major: Pervasive systems
Examiner: Professor Hannu-Matti Järvinen
Keywords: eMMC, IoT, IoT NAND, managed NAND, mass memory, memory

The thesis is written as a consulting assignment to Helsinki Memory Technologies Oy. The motivation for this assignment was to learn more about mass memories as a part of Internet of Things ecosystem. Additionally, the thesis seeks if there could be the potentially new business opportunities at the target field.

The thesis describes core technologies related to the solid state mass memories in the world of Internet of Things (IoT) at Chapter 2 to 4. Standards chapter covers the benefits of the standardization and the most important corresponding IoT forums. That chapter also summarizes IoT development activities of the key companies. At the end of the thesis there is an analysis of the new business opportunities found during the consulting period, which are grouped into two subsets: the extensions of existing solutions and the new IoT usage models with memory focus.

Conclusion chapter states that the architecture of managed NAND holds a strong position, which is foreseen to remain. This enables the development of IoT support to the mass memories. An additional conclusion is that IoT has reached the critical mass, but its final implementation is not defined yet. The business potential of IoT is estimated to be significant. These conclusions lead to recommendation for continuing studying the role of the mass memories in the IoT ecosystem. The final conclusion is that organizations, which study the implementation of IoT to the mass memory in details, will be well prepared and have an adaptable technical offer.

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan koulutusohjelma
FLOMAN, MATTI: Massamuistit ja laitteiden Internet
Diplomityö, 53 sivua, 1 liitesivu
Elokuu 2015
Pääaine: Pervasive systems
Tarkastaja: professori Hannu-Matti Järvinen
Avainsanat: eMMC, IoT, IoT NAND, managed NAND, massamuisti, muisti

Diplomityö on kirjoitettu osana konsultointi-toimeksiantoa, jonka tilaaja on Helsinki Memory Technologies Oy. Työn tarkoituksena oli selvittää puolijohteista valmistettujen massamuistien roolia osana Internet of Things:ä (IoT). Lisätavoitteena työllä oli esitellä uusia tapoja käyttää edellä mainittuja muisteja.

Työn alkuosassa kuvataan aiheen mukaiset ydinteknologiat. Teknologioiden esittelyä seuraa standardointi-luku, jossa tuodaan esiin toiminnan edut ja haitat sekä merkittävimmät standardointiorganisaatiot. Luku sisältää myös lyhyen katsauksen tärkeimpien IoT-kehittäjien viimeaikaisista toimista. Työn loppuosassa analysoidaan työn tekemisen myötä syntyneet uudet käyttötavat massamuisteille. Käyttötavat on luokiteltu kahteen ryhmään, jotka ovat nykyisten ratkaisujen parannukset sekä uudet IoTiin perustuvat ratkaisut.

Loppuyhteenvedossa managed NAND-arkkitehtuurin vahvan roolin nähdään jatkuvan. Kyseinen arkkitehtuuri mahdollistaa IoT-tuen toteuttamisen massamuisteihin. Yhteenvedossa IoT:n katsotaan saavuttaneen kriittisenmassan, mutta IoT:n lopullinen toteutusmuoto ei ole vielä tiedossa. IoT:n liiketaloudellinen potentiaali arvioidaan erittäin merkittäväksi.. Näihin syihin perustuen yhteenveto suosittelee tutkimaan massamuistien IoT-roolia tarkemmin. Organisaatiot, jotka tutkivat mahdollisuuksia massamuistien IoT-tuen toteutukselle, ovat hyvin valmistautuneita tulevaisuuteen sekä tarjoavat joustavat tekniset ratkaisut.

PREFACE

The thesis is written as a consulting assignment to Helsinki Memory Technologies Oy. The motivation for this assignment was to learn more about mass memories as a part of Internet of Things ecosystem. Additionally, the thesis seeks if there could be the potentially new business opportunities at the target field.

The author has sixteen years' extensive work experience related to the development of the mobile mass memories. The responsibilities evolved during these years from the technology specialist to the technology manager. The writer has wide experience in the technology standardization via participation in the technical works on the committees and multiple board memberships. Work experience has included close long term cooperation with major chipset and memory manufacturers. Author also worked as an adviser related to Machine to Machine (M2M) development activities.

TABLE OF CONTENTS

TERMS AND DEFINITIONS

BIST	Built-In Self-Test is procedure, which in integrated to the device for automated testing.
cloud	Computing architecture, which emphases the role of the global computing.
DRAM	Dynamic Random Access Memory is volatile memory, which is typically used as main memory of the device.
EEPROM	Electrically Erasable Programmable Read-Only Memory is non-volatile memory, which supports random access,
ECC	Error Correction Code is a method for fixing founded errors in data, which has been loaded from the used storage media.
eMMC	Embedded mass memory, which originates from MMC memory card. Typically eMMC package includes combination of NAND flashes and separate controller chip.
ETSI	European Telecommunications Standards Institute.
fog	Computing architecture, which emphases the role of the local computing.
IEEE	Institute of Electrical and Electronics Engineers.
IEFT	Internet Engineering Task Force.
IERC	European Research Cluster on the Internet of Things.
IoT	Internet of Things is a network of wide range of devices, which automatically exchanges information. Each device has individual ID.
IoE	Internet of Everything is based on IoT and according to Cisco IoE introduces additional network intelligence compared to IoT. Cisco is also defining that IoT is connection between physical devices as in case of IoE they do list also people.
IPR	Intellectual Property Right.
JEDEC	JEDEC is standard organization focused to microelectronics industry.
LWM2M	LightWeight M2M is a communication protocol to be used between M2M device and M2M server. It is defined by OMA.
Managed NAND	Mass memory architecture, which consist of NAND flashes and separate controller chip.
MLC	MultiLevel Cell, NAND flash technology in which one memory cell is used to store multiple data bits.
M2M	Machine to Machine is a subset of IoT, which emphasizes that connection is between devices not “things”. Based on

	author's experience of reading articles related to M2M and/or IoT, these terms are often used for same meaning.
NAND flash	Non-volatile memory, which name comes from NAND gate. NAND flash can be of two main standards, which owners are ONFI and JEDEC.
NAS drive	Network-Attached Storage drive is mass storage device, which is accessed via Internet. Typical NAS drive consist of backplane with slots for hard drives.
NOR flash	Non-volatile memory, which name comes from NOR gate. Instead of strong standard NOR flashes have multiple manufacturer/user specific solutions.
XIP	Execute In Place, memory architecture in which code is executed directly from the non-volatile memory.
OMA	Open Mobile Alliance is standard organization focused to mobile solutions.
PDA	Personal Digital Assistant, electrical devices which is typically small enough to be held in hand. These devices provide functionality of the small computer.
PSRAM	Pseudostatic Random Access Memory is volatile memory, which is based on DRAM cell technology, but has SRAM interface.
RFID	Radio-Frequency Identification technology is used for transferring identification information between reader and tag
ROM	Read Only Memory provides only read function. Content of the memory cannot be changed.
SDA	SD Association is standard organization focused to memory card standards.
Shadowing	Memory architecture in which code is loaded from the non-volatile memory to the volatile memory for the execution.
SLC	Single Level Cell, NAND flash technology in which one memory cell is used to store only one data bit.
SOC	Silicon On Chip, widely used acronym for central processing unit of the mobile device.
SSD	Solid State Disk, functions as a hard drive, but instead of rotating magnetic media data is stored to solid state memories.
UFD	USB Flash Drive is mass memory, which connect to Universal Serial Bus port.
UFS	Universal Flash Storage is next generation mobile mass memory standard defined by JEDEC.

USB	Universal Serial Bus is serial interface standard, which defines connection between personal computers and other electrical devices.
USB OTG	Universal Serial Bus On-The-Go is variation of basic USB. This version of the interface introduces possibility to changes role of the device between the master and slave modes.
WiFi	Wireless local area network standard, which is defined by IEEE.

1. INTRODUCTION

The traditional mass memory implies the local device, which is used for storing the operating system, applications and user data. Development of the network interfaces has changed this approach. Fast and widely available Internet connections have introduced the network drives, which are available for all users. The global access is a major change for the user experience compared with traditional local mass memories usage. Another impact of the Internet access is the increased popularity of the Internet of Things (IoT). IoT was introduced by the group of MIT professors about 20 years ago. They defined connection and data sharing between things, which include devices and sensors. (Edson, 2015) This concept is based on the architecture where all electrical devices not just the computers are connected to Internet.

Microsoft states that IoT is at inflection point because of multiple reasons. While hardware cost is falling the number of devices communicating to each other is increasing. Variations in communication methods for IoT have increased once cellular networks become widely available with reasonable pricing additionally to earlier wired and wireless local area networks. Similar development has happened at cloud technologies. The last reason what Microsoft gives is economic potential of IoT. (Edson, 2015) Additionally to reasons pinpointed by Microsoft also other technology development advancements like lower power consumption, miniaturization and increased processing power have partly made IoT to be possible. At the same time as technologies have been advancing also new use cases have emerged and that has impacted to the emerging of IoT.

The definition of the computer has become wider due to development of the smart phones and tablets. They have impressive processing power, which make them competitors to low end desktops and laptops. In device volumes smart phones have already passed desktops and the cap is increasing (Danova, 2014). So, mobility has the important and extending role nowadays. Because of that mass memories in this thesis are primarily approached from mobile aspect.

Mobile computing has been strongly driving the development of the local mass memories. As the end result in the smart phones, small density Execute In Place (XIP) flashes have been widely replaced by managed NAND solutions. Similar type of the solutions is used in the tablets. The same development is happening at laptops and desktop computers where traditional hard drives are replaced by solid state disks and modules, which are one type of managed NANDs. Managed NAND solutions are also used at the servers.

This new highly connected environment for mass memories is partly existing and partly is still developing. This thesis provides the required backgrounds of IoT, solid state mass memories and their existence in IoT ecosystem today. The background of IoT does covers technical aspects, standardization and development forums. Standardization and development forums were included in the thesis at the later phase. Motivation for this was that during studies it became clear to author as also to the customer that definition of IoT and its main use cases are not clear. IoT is based on the compatibility of the different parts of IoT ecosystem (IEEE, 2015) and therefore for successful IoT volume development international strong standards are required (Pattison, 2014). Without standards compatibility exists only within closed systems. It is worth consideration that this kind of closed ecosystem provided by, for example Apple or Samsung can easily be available worldwide and it can cover all layers of IoT architecture. However, it is unlikely that one company would be able to rule major part of the IoT ecosystem and therefore compatibility would not exist in optimum way.

Additionally to the IoT technology summary the thesis has two main intentions. The first one is to analyze the opportunities to extend and/or improve existing mass memory usage. The second one is to innovate potentially new IoT usage models with memory focus.

2. INTERNET OF THINGS

IoT is a wide concept, which typically means a global Internet based system, which consists of a wide range of devices. At the lowest layers, devices are simple, for example sensors and at the highest layers the complex devices like cloud masters are located. One driving force for IoT is its volumes. IoT devices are in use around the world as Figure 1 shows.

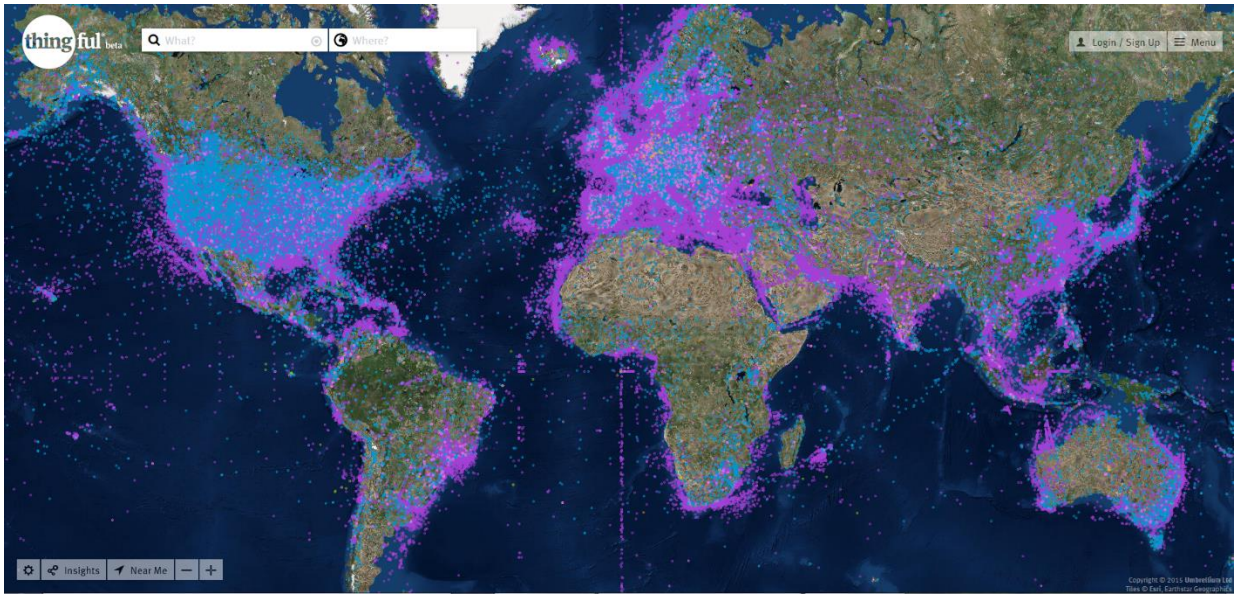


Figure 1Spreading of IoT devices (Umbrellium, 2015).

The highest concentration of IoT devices is in the most populated areas, but as IoT device range is wide they exist around the world. The good example of this is ships, which are connected to Internet. Figure 2 compares IoT volumes with other devises connected to Internet.

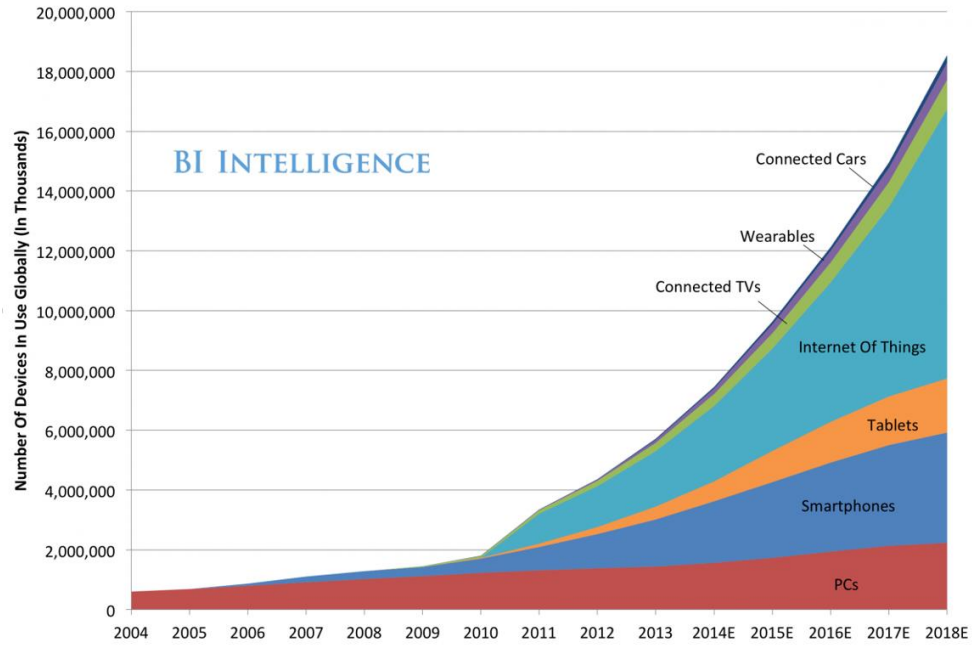


Figure 2 Volumes of devices connected to Internet (Danova, 2014).

Figure 2 is giving valuable information about volume differences between the most popular consumer computing devices. Smartphones are already more popular than PCs and difference will increase. Tablet volumes are likely increasing, but they will not match smartphone volumes. Based on the volumes smartphones are ideal local host products for IoT. Samsung shares the same trend message, but they do forecast even higher growth as can be seen on Figure 3.

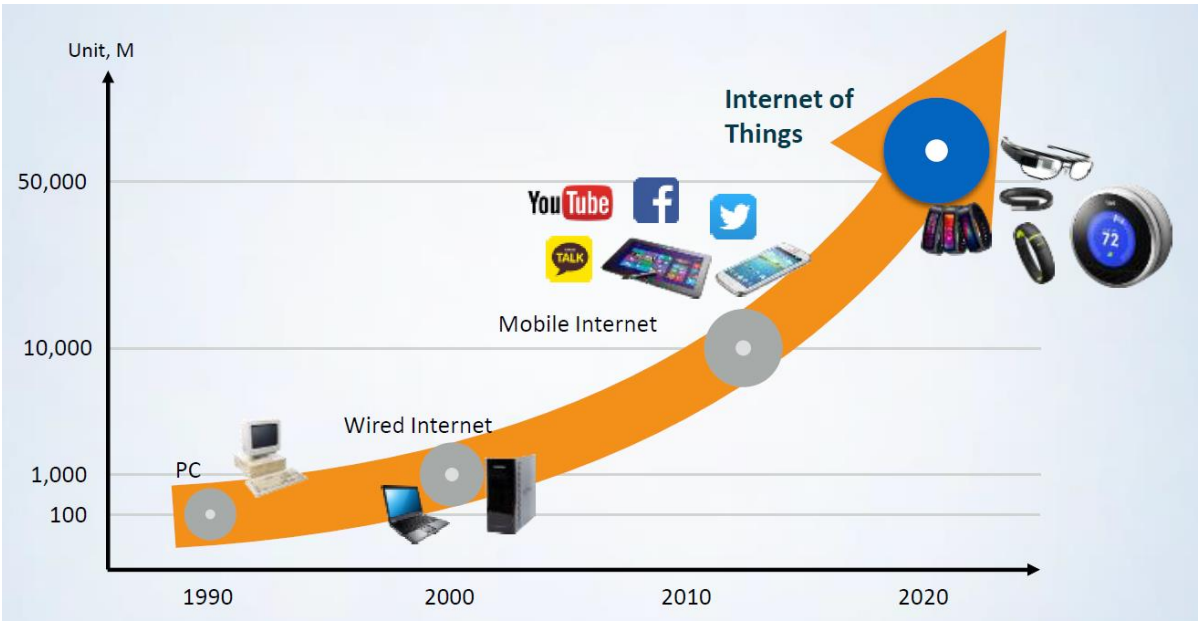


Figure 3 Volumes of the devices connected to internet according to Samsung (Elliot & Brennan, 2014).

Earlier Ericsson shared the Samsung's vision, but they have dropped volume estimation for connected devices in the year 2020 from 50 billion to 26 billion (Wood, 2015). Volumes are interesting as they do give an idea of potential value generated via them. Cisco is estimating that value generated by IoT will be 8 trillion USD during the next ten years (Noronha, et al., 2014). The forecast of how IoT semiconductor revenue is divided by industry is given in the Figure 4.

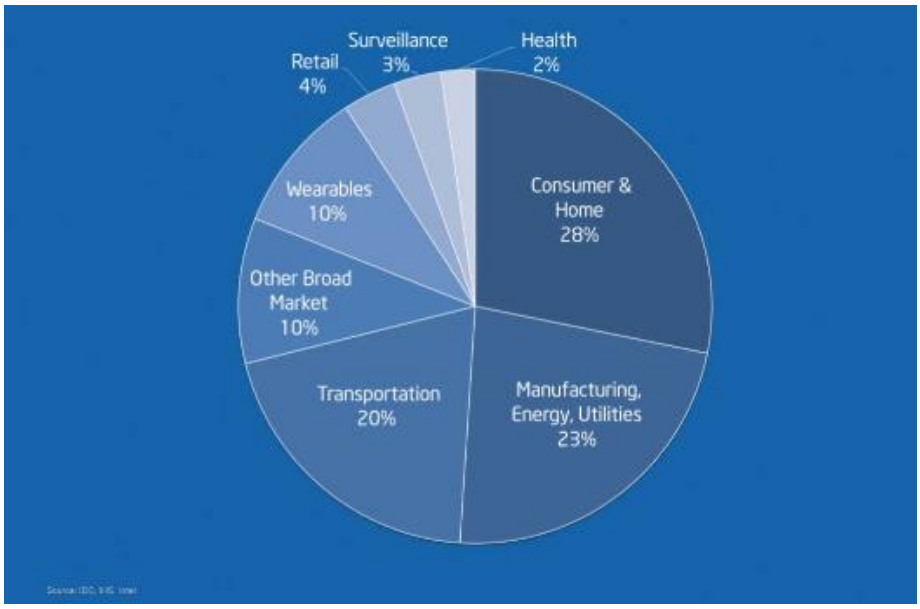


Figure 4 2020 IoT semiconductor revenue (Mcguirk, 2015)

Figure 5 gives a simplified idea why volumes of IoT devices are expected to be high. The wide range of use cases is clearly increasing potential of IoT, but it is also introducing a risk of having unclear scope. Institute of Electrical and Electronics Engineers (IEEE) study shares the vision of the wide range of use cases (IEEE, 2015).Attachment 1 shows the same in more details.

Figure 5 IoT environment (Mehraban, 2014).

There are multiple definitions for IoT. Additionally to IoT there are other concepts, which are close match to IoT. For example Machine to Machine (M2M) and Internet of Everything (IoE) are close relatives to IoT. According to Open Mobile Alliance (OMA) M2M is the subset of IoT (Klas et al, 2014). IEEE goes as far as pointing out that there is no official definition for IoT (IEEE, 2015). IoT related standard organizations are covered more in detail in Chapter 5.

For this thesis author has selected to use the definition by European Research Cluster on the Internet of Things (IERC). This definition is shown on Figure 6.

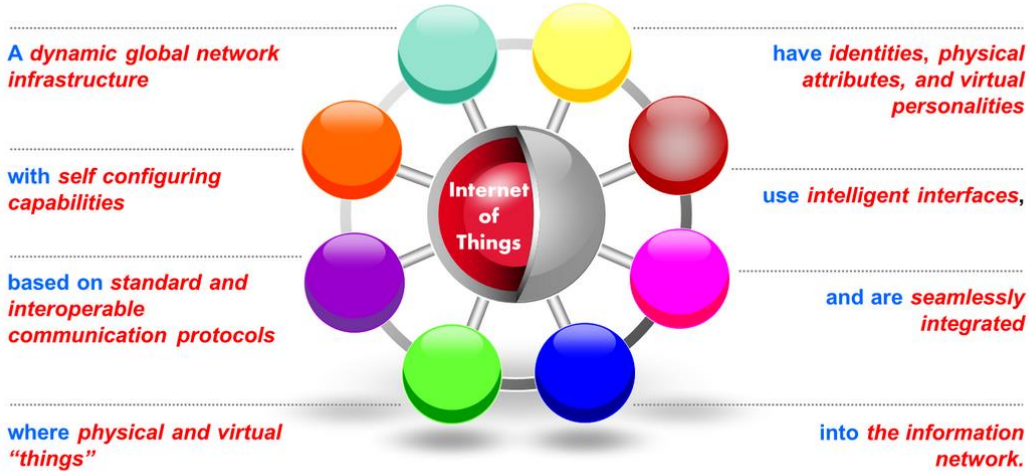


Figure 6 IoT definition (European Research Cluster on the internet of things, 2015).

Characteristics of IoT are the automatic operations (IEEE, 2015) at and between devices, which have unique IDs, the interface and the information transfer (European Research Cluster on the internet of things, 2015). The connection can be wireless or wired and, depending on the layer in the architecture, a wide range of protocols is available. Information can travel both directions and it can be processed depending on the use case at any layer. However typically processing happens at the higher layers while the lowest levels act as data collectors. An important aspect of the architecture is that IoT has much wider usage of horizontal connections compared to today's network setups as can be seen on Figure 7.

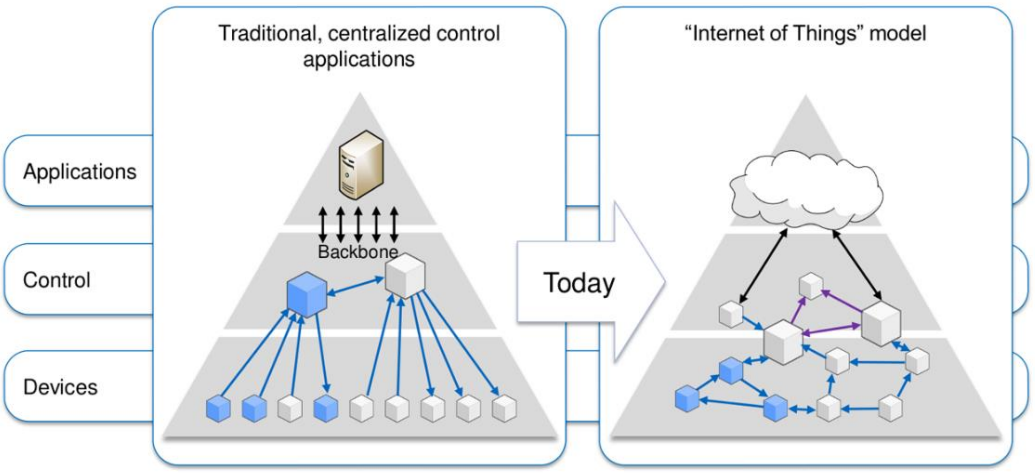


Figure 7 Architecture comparison (Vermesan, 2014) .

As one of focuses of this thesis is mass memories it is important to consider where data is stored and processed. IoT network does not limit computing location to be either local or cloud. IoT concept supports splitting computing to fog and cloud. (Noronha, et al., 2014).

3. SOLID STATE MASS MEMORIES

This chapter describes the development history, key parameters and different architectures of the solid state mass memories. Purpose of the chapter is to provide the reader with tools for understanding why solid state mass memories exist, what was driving the development and how today's technical solutions enable a natural way to support IoT.

3.1 Solid state mass memories development history

The size of digital universe doubles every year. Its density was 4.4 ZB in the year 2013 and it is estimated to reach 44 ZB in the year 2020 (Mcguirk, 2015). At the same time split between different storage media is changing as Figure 8 illustrates.

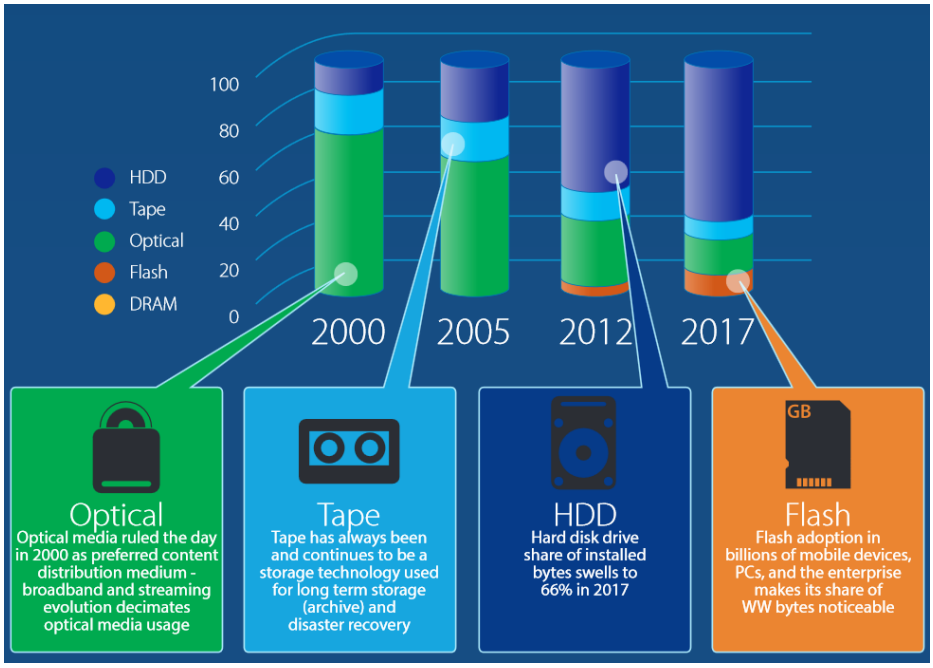


Figure 8 Installed bytes per media type (IDC, 2013).

Today de facto solution for solid state mass memory is managed NAND (Tsai, 2010); (Elliot & Brennan, 2014), which is based on NAND Flash. Managed NAND provides optimized solution for the wide range of products. There are two main groups of managed NANDs, which are Solid State Disks (SSD) aimed at PCs and mobile managed NANDs.

Before the era of smart phones NOR flash was used as a non-volatile memory storage at mobile products. Non-volatile memory does not lose its content once power in turned off. NOR flash was popular as it provides fast random access and does not

have similar failure mechanisms as NAND flash. New use cases like mobile imaging, video, music and advanced applications increased memory density requirements. Higher density requirements caused replacement of NOR flashes with NAND flash (Micron, 2013). Currently the market value of NOR flash is less than 10% of NAND flash market value, which was estimated to be 28 billion dollars in 2014 (MarketResearch.Asia Group, 2014). The memory density increase impacted to two key parameters. The first is availability of the needed density and the second is cost per bit. NAND flash provides better solution for high densities in both of these aspects. One reason why NAND flash provides much higher memory density is that its cell size is about half of the NOR cell size (Tal, 2003). Opposite to NOR's fast random access NAND is optimized for storing and moving sectors/pages vs. bytes as can be seen from Figure 9.

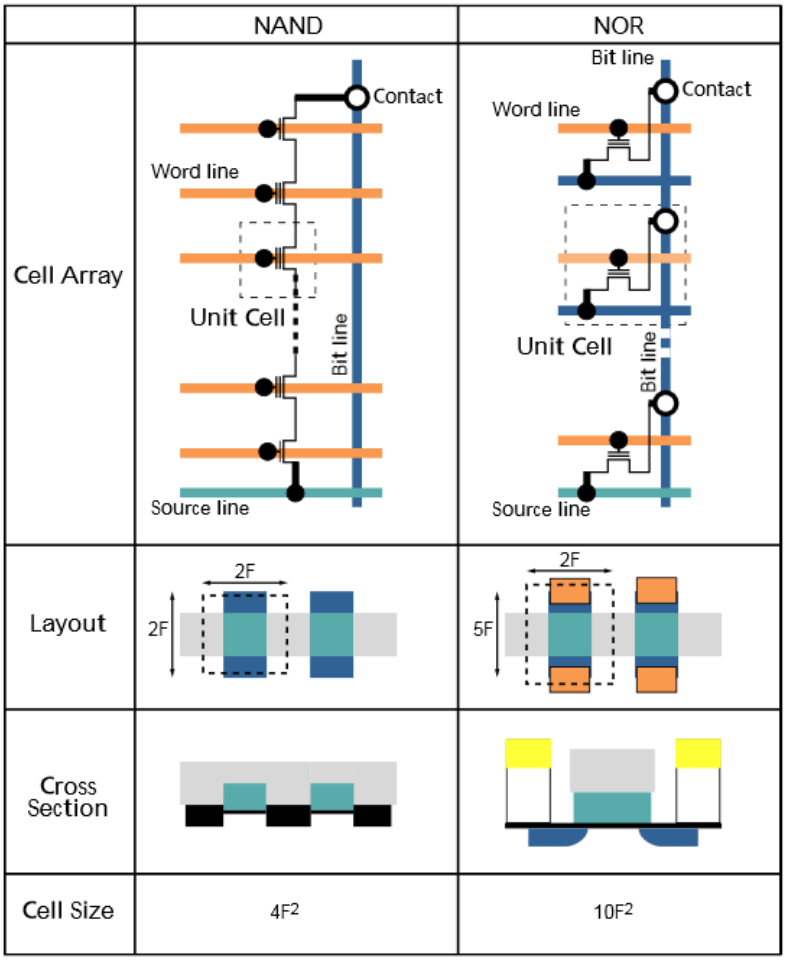


Figure 9 Differences between NOR and NAND (Micron, 2006).

Benefits and disadvantages of NOR and NAND flashes are shown on Figure 10.

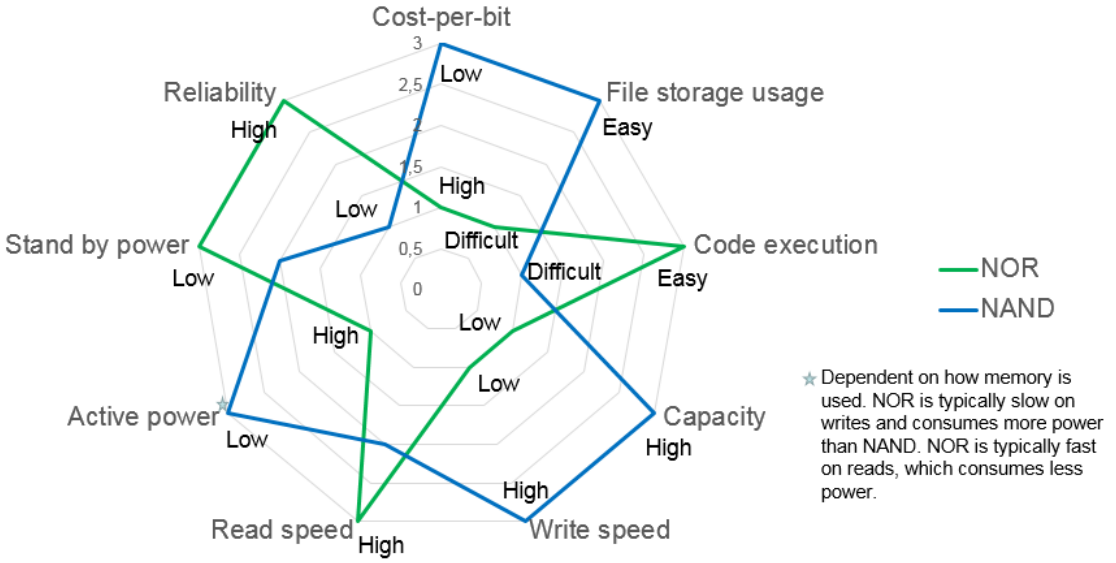


Figure 10 Differences between NOR and NAND flashes (Toshiba, 2006).

Original material by Toshiba did not present reliability aspect, which was included in Figure 10 since reliability is important driver for the managed NAND architectures. The reason for low score in case of NAND flash is its feature to have failures in the part of the cells during the usage. Some of these failures are permanent and some of them can be fixed. NOR flash does not have similar failure mechanism so it receives score three.

3.2 Different architectures

First NAND flash architectures had direct connection between the NAND flash and the Silicon On Chip (SOC). This solution has two names and they are pure NAND and raw NAND. Functionality is the same in the both cases and therefore only pure NAND term will be used in this thesis. The pure NAND architecture has required that the host devices manufacturer need to know how to manage each NAND flash, what he used. The NAND management includes the error correction, faulty block handling, wear levelling and the NAND flash design specific driver. The benefit of this implementation is that lower level functions, which are error correction, faulty block handling and wear levelling could be implemented by using the resources of SOC and memories connected to it. Once the Single Level Cell (SLC) NAND flashes were used NAND management was already challenging, but the introduction of the Multi-Level Cell NAND flash made this very difficult as all changes were visible directly to the host system. The future of the NAND flash is not yet fixed (Handy, 2014) (Elliot & Brennan, 2014) (Kilbuck, 2014). Therefore it is very difficult to forecast exact requirements for the host system in case of pure NAND implementation. Even the smallest changes in the NAND design might require changes to the host software. The bigger challenge is that only small

changes can be balanced with host software and therefore all the bigger changes in the NAND flash design require changes to the SOC. In case of error correction implementation at the host system, the host manufacturer has to make the best guess concerning error correction requirements as this information is not always available on time. If this guess is wrong and the optimum NAND flashes available at the market during the life time of the host system would require higher error correction than implemented these flashes would not be usable without changes. Change to the host unit once it is already at the mass production is typically something what host manufacturers avoids due to the risk in schedules. Therefore the manufacturer might continue to use non optimum NAND flash. The continued usage of the non-optimized component might lead to a higher total cost or even in the worst case reduced life time of the host product due to lack of available NAND flash. The selection to implement needed changes to the host unit requires additional development investments and might impact also to the production schedules. An additional challenge of pure NAND approach is that cost optimized NAND process used to manufacture the NAND memory is the limiting factor for the logic used for the interface as also for other potential features.

The solution was adopting managed NAND architecture from memory cards. Managed NAND architecture hides actual NAND memory implementation by having separate controller chip inside the mass memory module. Added controller chip is processing in the background the lower level NAND management functions, which earlier were loading host systems. The controller chip is also doing needed protocol translation between the NAND memory and SOC. The separate controller chip allows the usage of the optimal logic process for the controller and the optimal memory process for the NAND flash. This way functionality of managed NAND can be scaled up if impact on-cost structure is justified. Moving to managed NAND was not straight forward step as there were multiple computing solutions, which provide a mixture of features between pure NAND and managed NAND. At the end benefits of managed NAND made it a winner. These benefits can be seen on Figure 11.

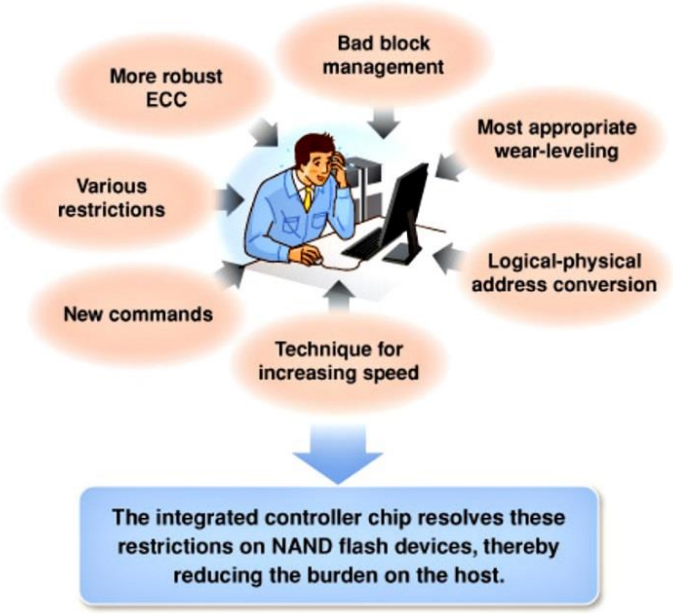


Figure 11 Benefits of managed NAND architecture (Toshiba, 2014b).

Figure 12 shows how the architecture of the mass memory changes and what are the key benefits once pure NAND architecture is replaced with managed NAND architecture.

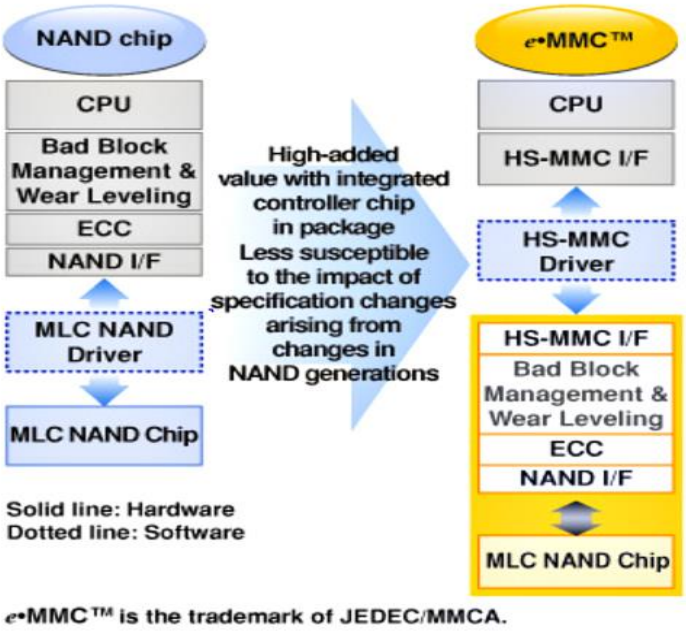


Figure 12 Move from pure NAND to managed NAND (Toshiba, 2014a).

According to Samsung's forecast NAND flash usage is growing heavily as Figure 13 shows.

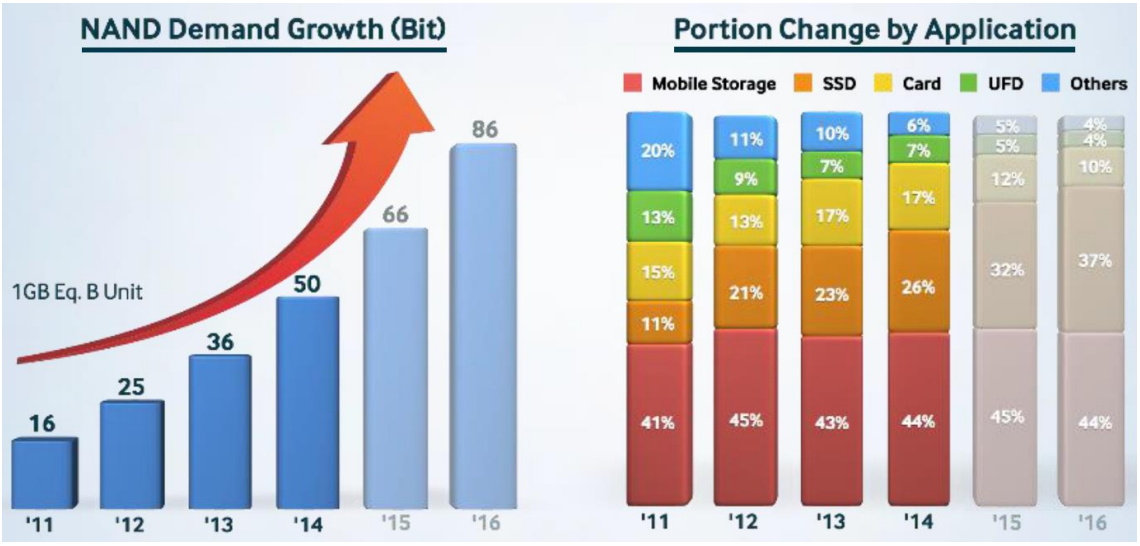


Figure 13 NAND flash demand and usage (Elliot & Brennan, 2014).

SSDs have better performance and higher budget for power consumption and cost, but from the architecture point of view they are managed NAND devices as can be seen from Figure 14.

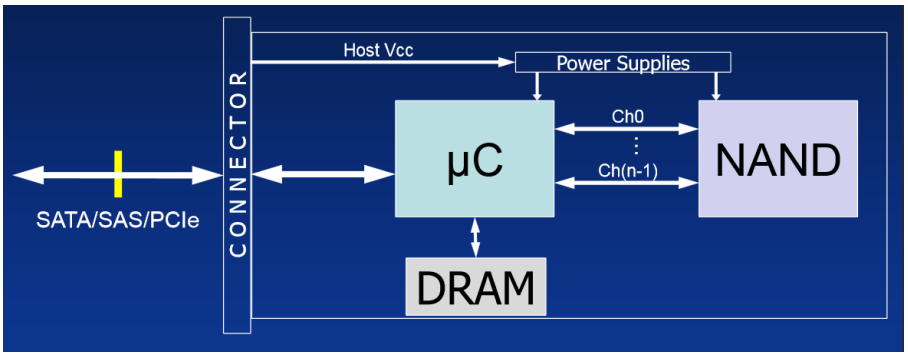


Figure 14 SSD architecture (Abraham, 2014).

The same applies to the Universal Serial Bus (USB) flash Drive (At Figure 13 USB is called UFD, which stands for USB Flash Drive) (Abraham, 2014). Major part of mobile storage is implemented by using managed NAND architecture as stated earlier. Therefore managed NAND architecture is the solution for major part of the whole NAND business. There are indications that pure NAND architecture might not be available in the future as even designs which use pure NAND interface are starting to have a separate controller as shown on Figure 15. According to Toshiba modern NAND flash's Error Correction Code (ECC) requirements and performance motivates moving in this direction (Toshiba, 2015). Another reason could be that pure NAND providers and host manufacturers are making preparation for the unclear future of NAND flash. It is also possible that NAND manufacturers do not want to relieve details about advanced control methods required for their new multilevel cell (MLC) NANDs and therefore prefer to hide them by using a separate controller.

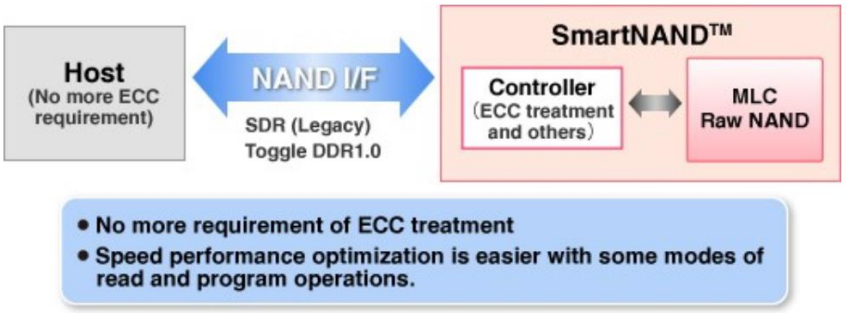


Figure 15 New pure NAND trend (Toshiba, 2015).

An important development trend in the managed NANDs and especially in case of the mobile managed NANDs is the increasing role of functionalities, which are not purely memory access related. This concept of not purely memory access related functionality is authors attempt to point out that mentioned functions are not mandatory from the basic memory usage point of view. So far these functions are improving the functionality, performance and usability of the host system. The concept is vague, but it is introducing a set of rogue functionalities which can be increased if business case mandate so. The typical limiting factor for the number of such functionalities is cost structure and difficulties in justifying a higher cost with enough tempting use case improvements. Therefore highly cost driven components as pure NANDs and memory card are having very limited amount of not purely memory access related functions. SD memory card for example does have content protection mechanism included (SD group and SD card association, 2013) as that was justified at the time by the business needs.

In case of mass memories, which are used to store a system image, amount of not purely memory access related functionality has been growing steadily. Universal Flash Storage (UFS)) memory for example provides many new functions, which allow the host system and mass memory operate more efficiently. Unified memory is one of these functions. Unified memory allows UFS to use host systems Dynamic Random Access Memory (DRAM) for its own purposes. In this case UFS memory is accessing system DRAM via UFS interface. Advanced boot support and command interleave are also good examples of extended host system support. Capabilities of managed NAND logic are primarily limited by the use case related cost structure. Therefore next generation mass memories can provide much wider non memory access related functionality when suitable use case is found. Figure 16 shows rough estimation for split between not purely memory related functionality and directly to memory access related functionality over the latest mobile mass memory generations.

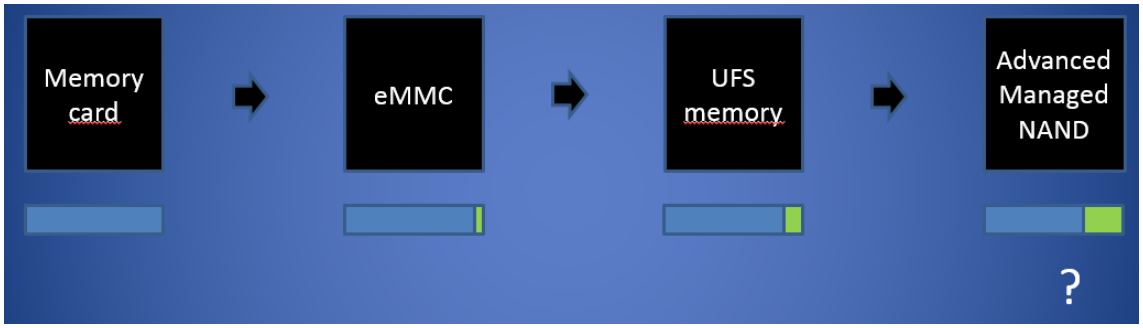


Figure 16 Growth of not purely memory related functionality.

At the Figure 16 the share of the additional functionality is marked with green compared with purely to memory related functionality. Question mark is emphasizing the fact that actual amount of non memory related functionality is highly depending on the use case and the development of the solid state mass memory standards like UFS.

4. MASS MEMORIES IN TODAYS IOT ENVIRONMENT

The starting point for the consulting work was the figure of the focus ecosystem, which was drafted by Helsinki Memory Technology during the first meeting. This picture has then been modified by the author and latest version is shown on Figure 17.

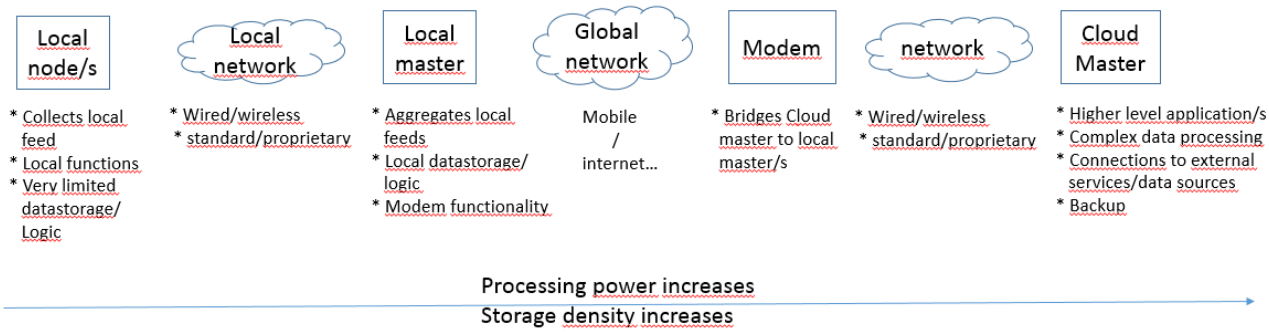


Figure 17 Topology of IoT environment (Mylly, 2015)

This description is very wide, but it is in line with other materials describing the ecosystem as can be seen later in Chapter 5.2 or on Figure 18.

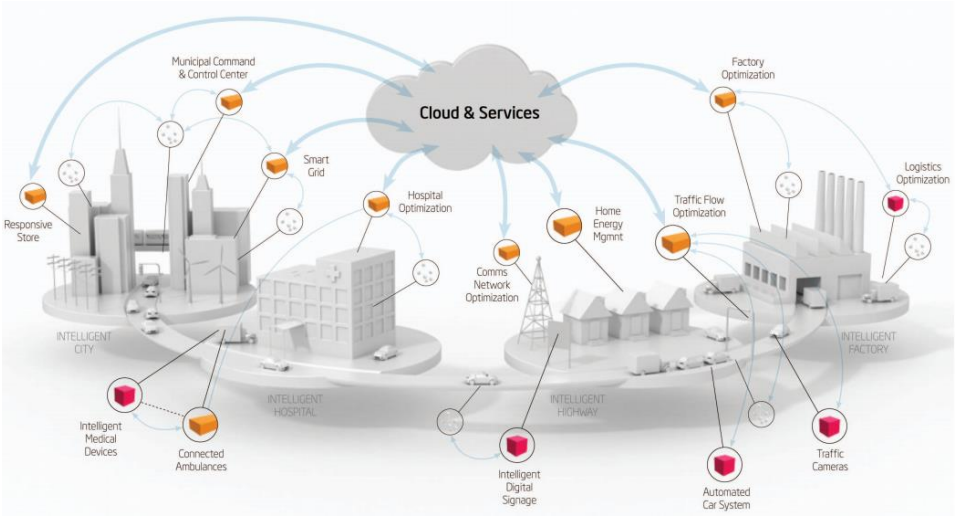


Figure 18 IoT based society (HUTGRIP, 2015).

One finding related IoT environment studies was that both available processing power and storage density increase once moving from the lower layer to the higher layer.

4.1 Implementations of IoT ecosystem

IoT definition used in this thesis does not describe implementation in the details. Instead an architect of the certain IoT system has wide flexibility in the selection of the actual implementations. This is true for all layers of the ecosystem. Therefore an architect of the certain use case has almost full freedom to implement the best solution to meet the target business case and call the end result to be IoT based.

There is a wide range of potential local nodes. A Local node can be any device, which generates data automatically and is able to transmit that data onwards. Typically, data is generated by following some external parameter for example moisture in case of the moisture sensor. However, data can also be generated based on some internal process at the local node. An example of this could be an internal counter, which follows some critical internal parameter for example cycling in case of NAND flash. Often a local node is understood to be a simple device, but there are no rules preventing it from having advanced logic.

An aspect to recognize is that there is no absolute requirement for the local connection availability. This means that local node can have a continuous connection to the local master or connection can be available only part time. Mesh networks are an interesting way to provide a local connection. This type of connection is peer-to-peer type where the end node might be connected to Internet via multiple end nodes. More advanced mesh networks like Wirepas Pino, which is shown on Figure 19, provides automated local connectivity (Wirepas, 2015).

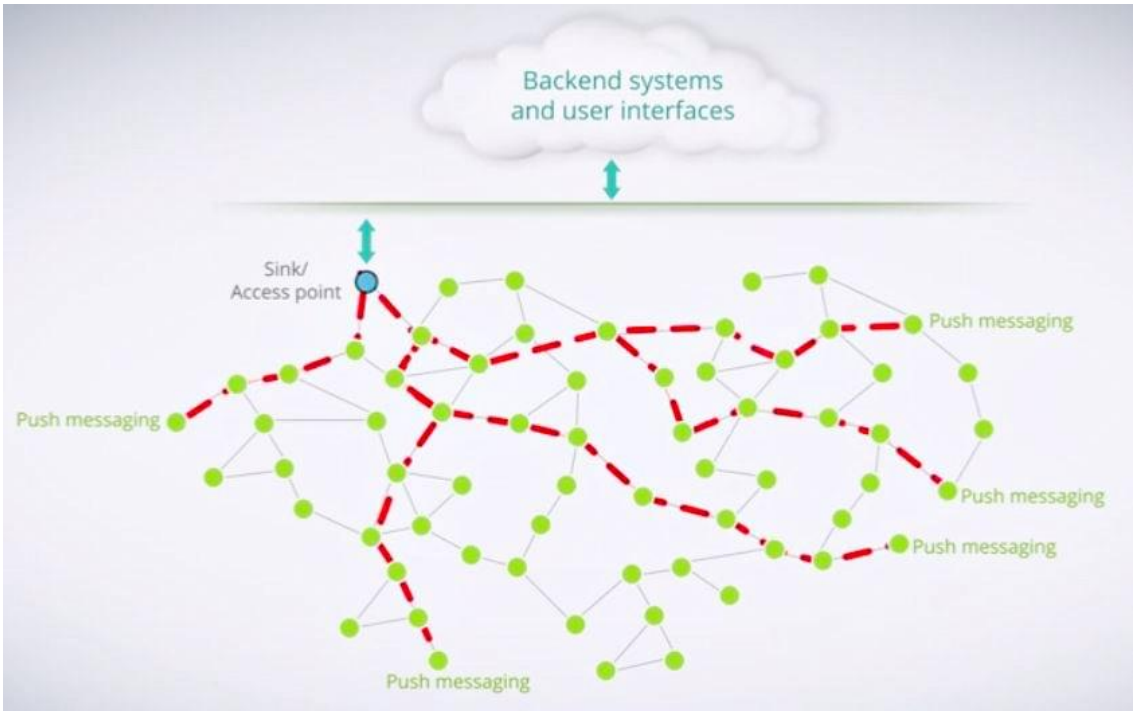


Figure 19 Wirepas Pino (Wirepas, 2015).

Another way to implement a local node's connection to IoT master is shown on Figure 20.

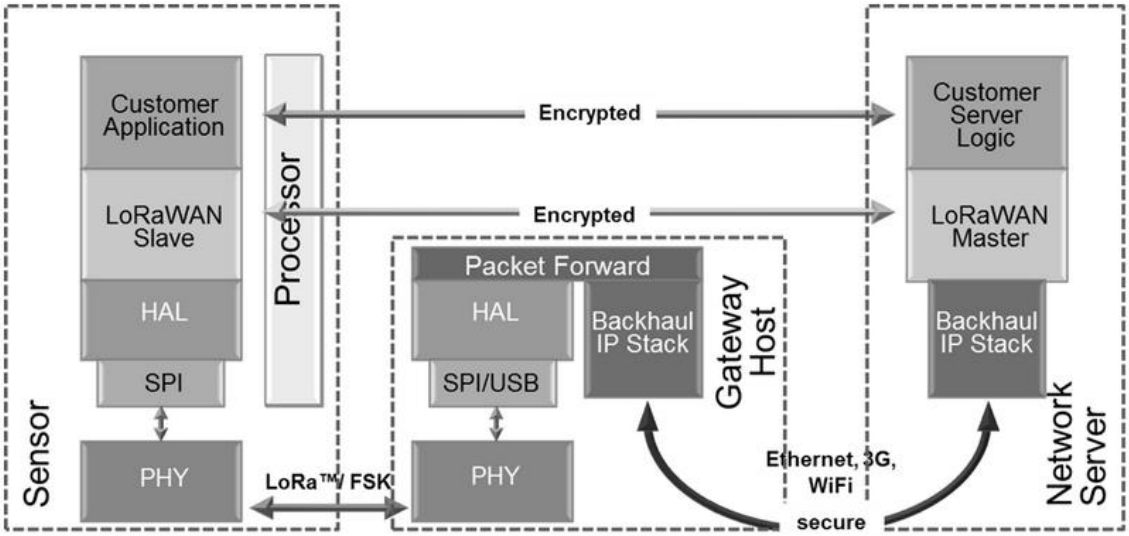


Figure 20 LoRa architecture (LoRa Alliance, 2015)

LoRa is a new wireless interface, which aims to enable low power and easy to use IoT functionality (LoRa Alliance, 2015). Instead of LoRa Bluetooth or any other suitable wireless or wire connection could be used to enable local network connectivity.

Similar way local master can have wide variation in the functionality. In the simplest implementation local master is just the router to Internet. It can also be a computer, what has a wide range of other functionality additional to IoT. It could be for example smart phone, which every now and then uses Bluetooth connection to download the latest moisture information from the local sensor node. This phone could then forward moisture data in raw format to Internet or it could store and/or process the data locally before sending it to Internet. The local functionality can also be fully included in one unit or there might be multiple local submodules. Figure 21 shows local master, which has connectivity as a driver.

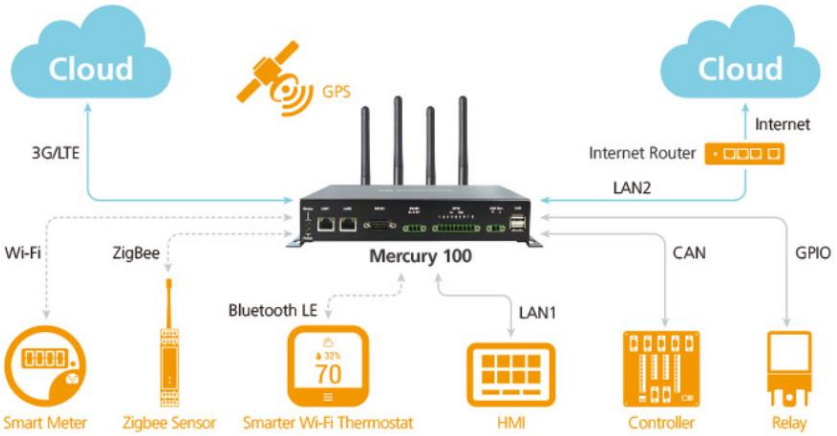


Figure 21 Local IoT master, which is focused to connectivity (Ambedded Technology, 2015).

The global network is the part of the ecosystem, which is the most finalized from the standardization point of view and still there are options. Local master can build

a connection to the cloud master or to the other local master by using mobile internet or normal wired Internet. Both of them have multiple generations in use so user needs verify existing support. For example if the local master uses 5G network and use place does not have coverage for that network then the system will not work. Of course one option is to provide downwards compatibility, but this might hit challenges for example in the bandwidth.

Modem functionality is needed on the cloud side also for connecting cloud to the global network. However, it is up to implementation if modem exists as a separate device. Should modem be a separate entity the network inside the cloud has to connect cloud master to the modem. Details of the actual implementations at the cloud servers are heavily depending on planned business size and available resources. At the simplest form, the cloud server can run at somebody's home and heavy duty servers have their own factory size buildings. The cloud server can have connections to other servers or it might also have connections to other devices like cellular phones via some other connection than wired or mobile internet. Typically, the cloud server is the place where all the data is collected for storing and processing. In case of IoT processing and storing can happen partly at lower levels and therefore IoT implements both cloud and fog computing as stated earlier.

Great flexibility defined above in case of IoT implementations for supporting business driven use cases increases the risk of the confusion. This confusion comes from the fact that today's term IoT does not guarantee compatibility between the actual devices. Therefore it is important to define all used protocols in the environment so end user knows exactly what the actual implementation is. Additional aspect to potential confusion gives estimations that number of IoT devices will be quite evenly divided between home, government/infrastructure and enterprise as can be seen on Figure 22.

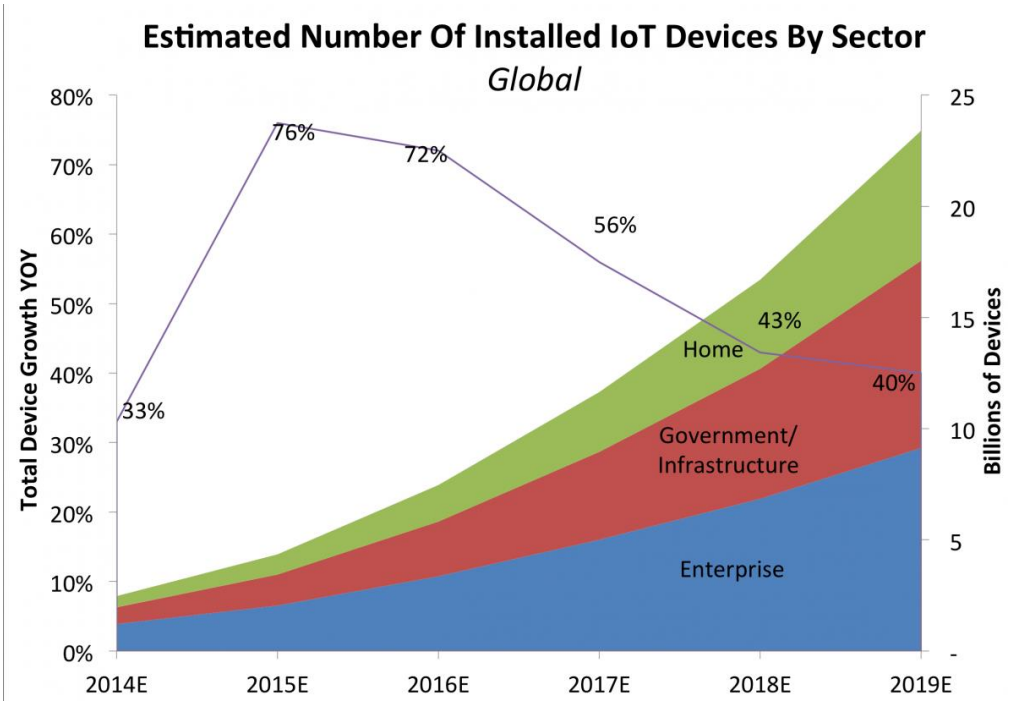


Figure 22 Estimated number of installed IoT devices by sector (Camhi, 2015).

Figure 22 demonstrates that IoT is in the middle of the steep volume increase. The challenge is that IoT standardization is still in the early phase as described in Chapter 5, but companies already make implementations. This might lead to high volumes of legacy products, which will not be fully or at all compatible with final IoT standards.

4.2 Mass memories in the IOT architecture

The local node's memory needs are depending on implementation. If the simplest sensor, which has a continuous connection to a local master, is implemented there is no need for mass memory. In this case only small non-volatile memory is required for settings, calibration and security parameters. Data buffering might also need small amount of the memory. However if connection type is mobile and local master is smart phone then the connection between the node and master is not available continuously. This kind of setup requires data buffering at the local node and depending on the amount of the generated data it might also need to be mass memory type. Typically **E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory (EEPROM) or NOR flash is enough for small data density needs. In simple node implementation key drivers for memory are physical size, low power consumption and cost. Power consumption and physical size are important as typical implementation is a small battery based device. Cost always has weight, but in case of simple devices, which might exist as multiple copies in one place, cost has increased importance. Security might be an impacting factor depending on the use case. Drivers like density and performance do not have an important role in case of simple implementation.

Local master has to be covered in two parts, which are fixed and mobile local master. Fixed local master needs to have storage for local data, operating parameters, operating system and potentially applications. Local data does not need to be fully stored to the master as it can be also forwarded to the cloud. Needed memory type is at minimum NOR flash and for higher memory needs mass memory based on NAND flash or hard drive is suitable. For fixed local master it is somewhat difficult to make assumption of the typical case as there is a wide range of implementations. In the average case the most critical driver can be security as data worth collecting is typically valuable. Density and cost also have reasonable weight. Performance is likely not the driver if only IoT aspect is approached. Should IoT be just one of the functionalities of local master then the importance of the performance is right away increasing. As fixed local master is typically connected to land line power consumption does normally have low importance. The role of power consumption might increase if IoT is just a part of the master's total functionality.

Mobile local master can have two different main implementations. It can work as local master, but this would mean that there is times once it might not be presented and therefore local nodes need to be able to tolerate this. The second implementation is that mobile master works on the top of the fixed master. In the later implementation local nodes will always have a connection to fixed master. Should mobile master exist

on the top of the fixed master, the role of mobile master is to provide advanced logic. It can also provide more personalized functionality if mobile master is smart phone. In both cases, most likely IoT functionality is just one of the features of the mobile master and therefore physical size, density, security, power consumption and cost have reasonable priority. Likely memory type would be managed NAND, which is used to store local data, settings, operating systems and applications.

The role of non-volatile memory in the modem, which is located to the cloud is small, since data would not be stored to modem and therefore memory needs to be able to store only settings, operating system and in some cases applications. Modem would be connected to fixed power so power consumption is not the driver. Security might have an important role.

Cloud master is typically the highest layer in the IoT ecosystem. Its role is to store the data received from lower layers and process the data. Received data can be raw data from the local node or it can already be partly processed data. In some cases, all data is not rising to the cloud master as it stays in lower layers. Typically, cloud master requires massive data storage, which is often implemented with numerous hard drives or SSDs. Since cloud master processes huge amount of important data all parameters are critical. The energy consumption and cost are critical because the number of memory devices works as a multiplier. The density requirement is only limited by the available economic resources. Nowadays there are cloud masters designed for small companies or homes, which can survive with similar mass memory needs as advanced PC. In this case limited number of hard drives or SSD will serve the need.

4.3 Memory architectures

To implement memory use cases described in chapter 4.2 two main architectures are used. These architectures are Execute In Place (XIP) and Shadowing. XIP is traditional mobile phone architecture, where code is executed from NOR flash and Pseudostatic Random Access Memory (PSRAM) is used as main memory. Increased density requirements have caused many XIP systems to have additional NAND based mass memory. Should XIP usage continue it is likely that over the time flash will move to DRAM interface.

Shadowing is architecture, which has been used in computers for long time and it came to mobile devices with smart phones. In case of shadowing architecture Code is downloaded from mass memory to the DRAM for execution. Shadowing provides high performance and it is optimum solution once interleaving/pipelining is used. Figure 23 shows different memory architectures.

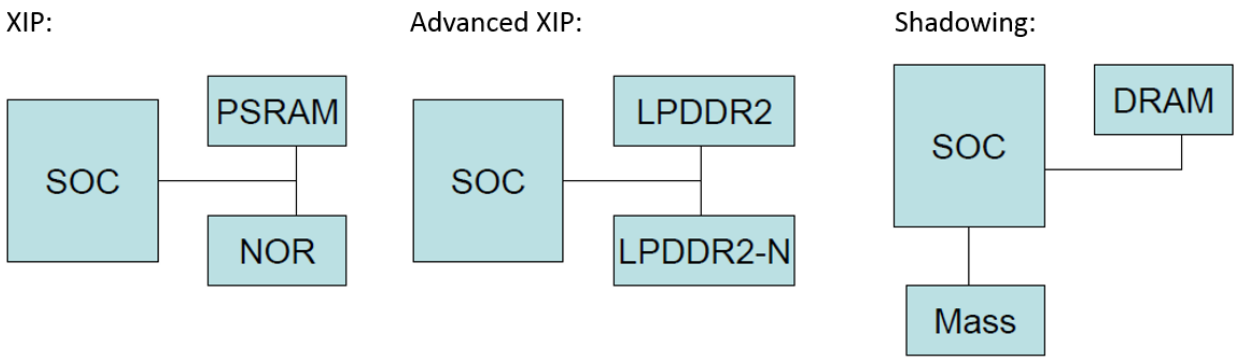


Figure 23 Memory architectures (Floman, 2012).

The common connection method for the local mass memory in today's systems is the direct connection. In this case mass memory is operating as the slave to the host device. Even if the host device would be IoT device, mass memory would not be seen directly by the other IoT devices. Figure 24 shows the simplified version of this kind of setup.

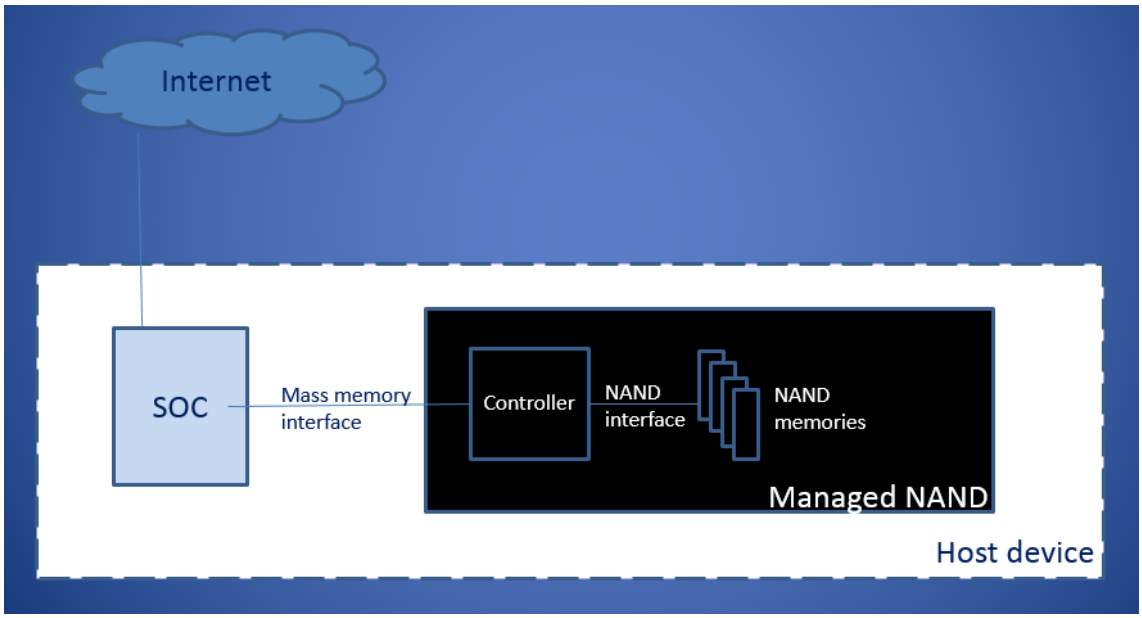


Figure 24 Traditional connection of local managed NAND.

In this setup all mass memory related activities visible outside of the mass memory module are controlled by the host device. This means that use cases based on focused control of mass memory are not supported as the host device has full control of data stored to mass memory.

5. STANDARDS

The main purpose to have standards is to enable compatibility. Standards make it possible to have ecosystems consisting of multiple entities, which can be connected together in the predefined way. In the simplest form, this is a master/slave connection by using the standardized interface. The critical aspect of an ecosystem of this kind is that it makes possible to have multiple suppliers and users, who all benefit from the prosperity of the ecosystem. This way market size of the ecosystem has optimum opportunity to grow.

The second essential reason to do cooperation at standard forums is the optimum usage of resources. If one company is doing development work, available resources are tightly limited. The same case is for available knowhow. Once the companies get together and develop a new standard in cooperation resources and knowhow limitations are not so bad an obstacle. The important thing to notice is that in the optimum case standard organization has mixed membership in other word it has members with different roles like the component manufacturer, the host manufacturer and the software company. This gives good visibility to the whole life cycle of the technology and therefore it is possible to define a standard in the optimum way. Wide visibility to the technology status and to the future needs via wide member base allows starting standardization activities much before the planned mass production. This enables members to reach the mass production earlier (Floman, 2012). Additional aspect related to know-how is that organized way of cooperation at standard forums provides the opportunity to maximize learning curve impact.

Major benefit of the standard organizations is the written bylaws, which guides the work. Predefined and optimized rules make efficient cooperation possible. When bylaws exist risk for conflicts is minimized and in the case of challenges there is a clear way to solve them. For example voting rules makes clear who are allowed to vote and how voting takes place. Well done bylaws cover also intellectual property rules for the standard organization. It is clear for all members, which way to handle potential patents including the notifications and the licensing rules. Some organization have bylaws, which guide avoiding the adoption of known Intellectual Property Rights (IPR) to the standards. It is common practice for the standard organizations to provide the list of the disclosed patents related to the certain standard. This is very valuable information and by itself good reason to be a member. Documented bylaws are also an easy way for potential new members to understand the organization and commitments involved in the membership.

Often standard organizations implement coordinated marketing activities. Marketing is an essential part of survival for the new solution. History has multiple cases showing that having best technical solution is not enough. For example MMC memory card had strong market leadership, but today's ruling memory card is SD card. SD Association (SDA) did make serious work at technical frontier to make this happen, but key activity was well coordinated marketing. Often new standards are supported by external marketing organization for maximum freedom to do marketing activities. For example Jedec's UFS mass memory has UFSA in this role (UFSA, 2015).

As justified above the standard organizations are a very strong tool for development work. However, they include several risks. One of them is power struggling inside the organization. This easily leads to delays in the schedules or not optimized technical solutions. Another risk is that entities inside the organization do not have clear focus, which can lead again to not optimized schedules and technical solutions. Sometimes there are multiple organizations focused on the same technology area. This might lead to market fragmentation and in the worst case this fragmentation can prevent any of these ecosystems from flourishing. Market growth might also be limited if the small number of companies have control of the ruling de facto standard or essential IPR portfolio.

5.1 Official IoT forums

One major finding during the thesis work is that there is not yet standard, which defines the whole ecosystem in detail. Neither does exist the upper level standard, which would collect required lower level standards to provide the whole standardized ecosystem. To understand the complexity of IoT and standardization related to it Figure 25 is introduced.

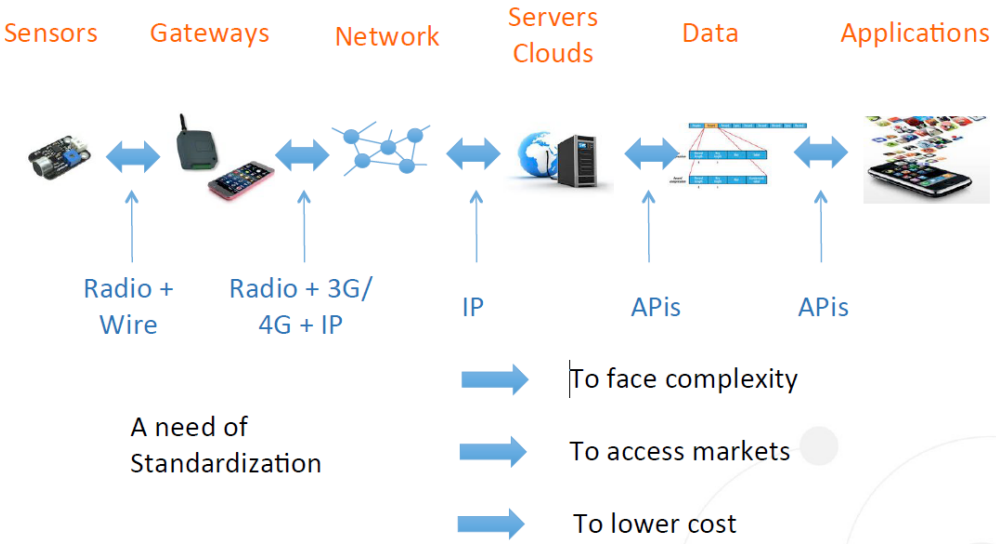


Figure 25 Standardization on the whole value chain (Rannou, H., 2014).

Current situation is quite confusing as media is full of articles about IoT, but even at the higher level there are differences in available IoT concepts as stated before. For example, IEEE's documentation includes people in IoT (IEEE, 2015), which is big difference compared with European Research Cluster on the Internet of Things's IoT definition, which includes only things. In other parts, there are a lot of similarities in these two descriptions.

Wide international cooperation is required to define the standardized IoT ecosystem. First key organizations ought to get together and agree about the goals and then more detailed work is required at each organization. IERC and European Telecommunications Standards Institute (ETSI) are listing many questions, open items and challenges, which have to be solved (IERC, 2014) (ETSI, 2014). They and different opinions of the key organizations show how challenging task IoT standardization will be. Open Mobile Alliance has tried to reduce silos between different solutions by introducing LowWeight M2M (LWM2M), which deployment scenario is shown on Figure 26.

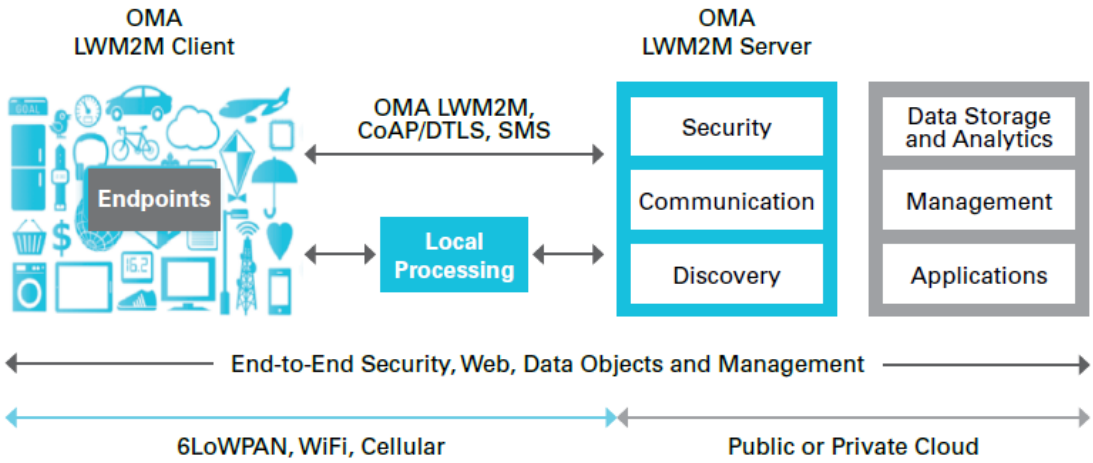


Figure 26 LWM2M solution (Klas et al, 2014).

LWM2M is adopted by some of the major industry players like Samsung and still Table 1, which shows key organizations listed by three different sources, does not include OMA. This makes it clear that there are major organizations missing from the list and still list includes already 14 organizations. Therefore it is obvious that standardization will be major challenge already at the cooperation level.

Source	IEEE	European comission	IERC
Organizations			
American National Standards Institute (ANSI)			Yes
European Committee For Electrotechncial Standardization (CENELEC)			Yes
European Committee for Standardization (CEN)			Yes
European Telecommunications Standards Institute (ETSI)		Yes	Yes
German Institute for Standardization (DIN)			Yes
Institute of Electrical and Electronics Engineers (IEEE)	Yes	Yes	Yes
International Electrotechnical Commission (IEC)	Yes		Yes
International Organization of Standardization (ISO)	Yes	Yes	Yes
International Society of Automation (ISA)	Yes		
International Telecommunication Union (ITU)	Yes		Yes
Internet Engineering Task Force (IETF)	Yes	Yes	Yes
Object Management Group (OMG)			Yes
Open Geospatial Consortium (OGC)			Yes
World Wide Web Consortium (W3C)	Yes	Yes	Yes

Table 1 Key IoT standardization organizations (IEEE, 2015) (IERC, 2014) (Campolargo, M., 2014).

It is good to remember that forums defined in the table 1 do not include multiple activities driven by major companies like Intel, Google and Samsung. IERC presents its own opinion about standard organizations and their roles on Figure 27.

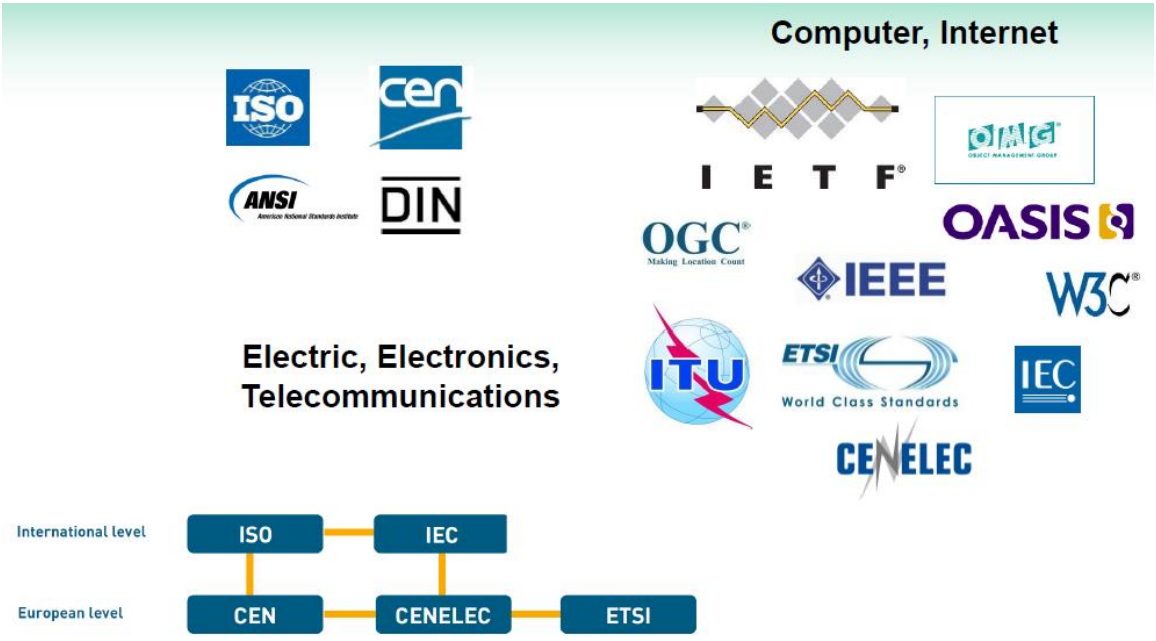


Figure 27 IoT standardization organizations (IERC, 2014).

5.2 Business driven IOT forums

Appinions was ranking the most influential IoT companies and results are shown in Figure 28.

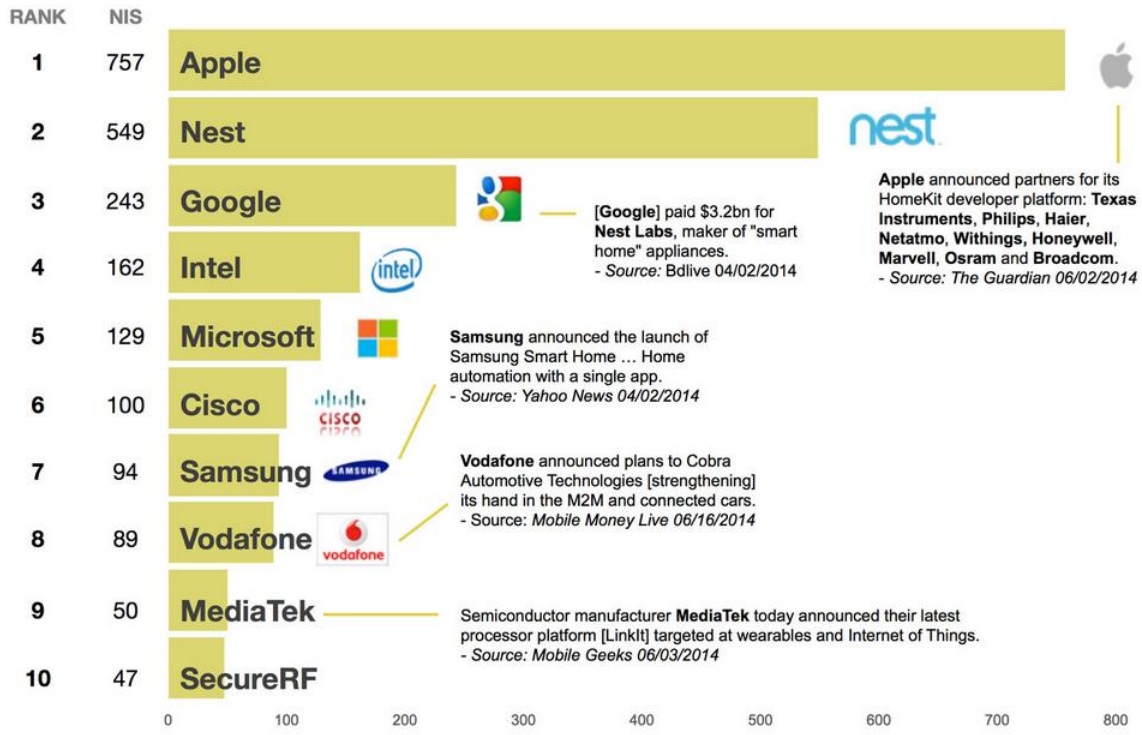


Figure 28 The most influential IoT companies (Appinions, 2014).

First seven companies are covered in the following subchapters. These companies have different approaches depending on the company strategy and resources. Based on publicly available information business driven activities can be divided into two main groups, which have cloud and ecosystem focus. Microsoft is an example of the cloud approach as Google, Intel and Samsung are examples of ecosystem emphasis.

5.2.1 Apple

Apple is the only one of these seven IoT companies whose public web pages do not get search hits when searching is done with company name and word IoT. Still Apple is the world's biggest company with business value and it holds a very strong position at the high technology not to forget Apple's extensive capital resources. Therefore it is not surprising that Apple is active at many areas, which are closely related to IoT like mobile devices, laptops, tablets and cloud services. They have also announced their own solution for device communication and control at users home. Apple is calling this solution as Homekit. In Homekit setup user stores local Homekit devices to IOS device, which content is then synchronized with Apple cloud. With IOS devices, user can control Homekit accessories either locally or remotely. (Apple, 2015) First Homekit accessories are now available (McGarry, 2015)

5.2.2 Google

Google's approach to IoT was to support it as solution via Google Cloud Platform, (Google, 2015a). Google Cloud Platform provides customers with access to

Googles extensive resources like its private global network, good at redundancy and access to the latest technologies and more. One available resource, which is close to the title of this thesis work is range of cloud storage services. (Google, 2015b) Google acquired Nest in February, 2014 and increased its own strength in IoT area (Appinions, 2014).

Google announced on May 28th 2015 their new approach to IoT. According to Google fundamental building blocks for IoT are the operating system, communications and user experience. The underlying operating system is project Brillo (Pichai, 2015), which architecture is shown on Figure 29.

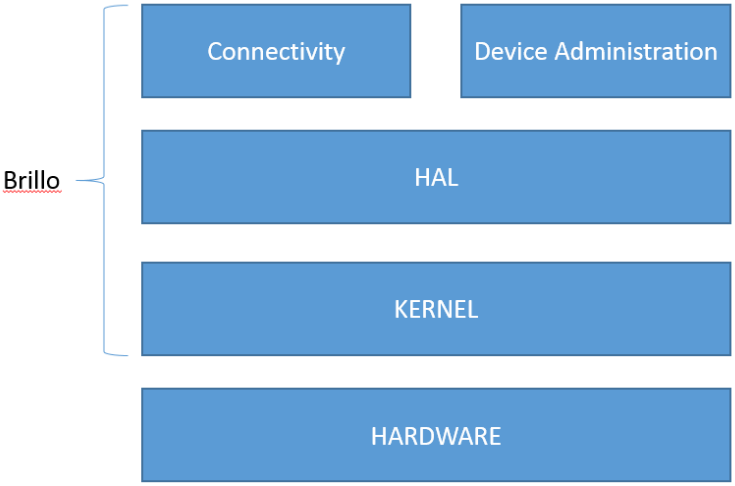


Figure 29 Brillo operating system (Pichai, 2015).

Brillo is derived from Android and therefore installation based of Android is available. According to Google Brillo sets minimal system requirements. Google has used both Android and Nest R&D people to provide end to end solution to IoT. For communication layer Google uses Weave, which is the communication protocol between all of the devices as shown on Figure 30. (Pichai, 2015)

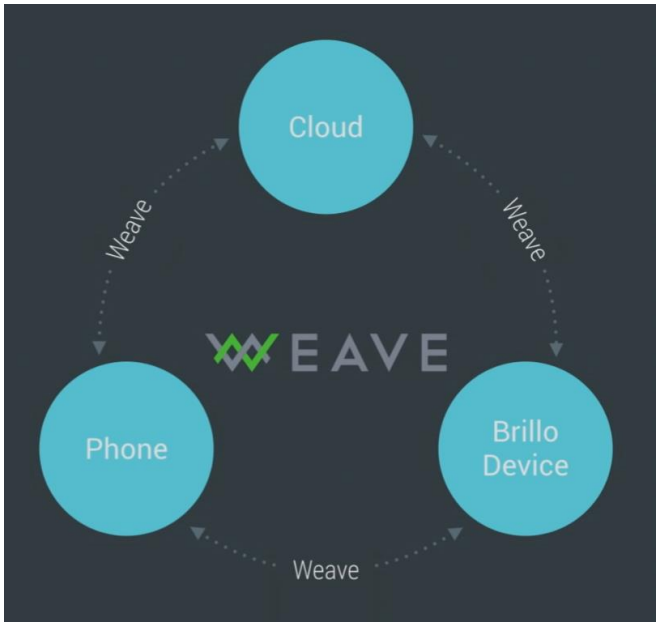


Figure 30 Weave communication protocol (Pichai, 2015).

As Brillo is based on Android and Weave is used in all devices, any Android device can be employed as a user interface to control IoT devices based on Google's solution (Pichai, 2015).

5.2.3 Intel

Intel is providing solutions to their customers to each level of IoT ecosystem as Figure 31 shows.

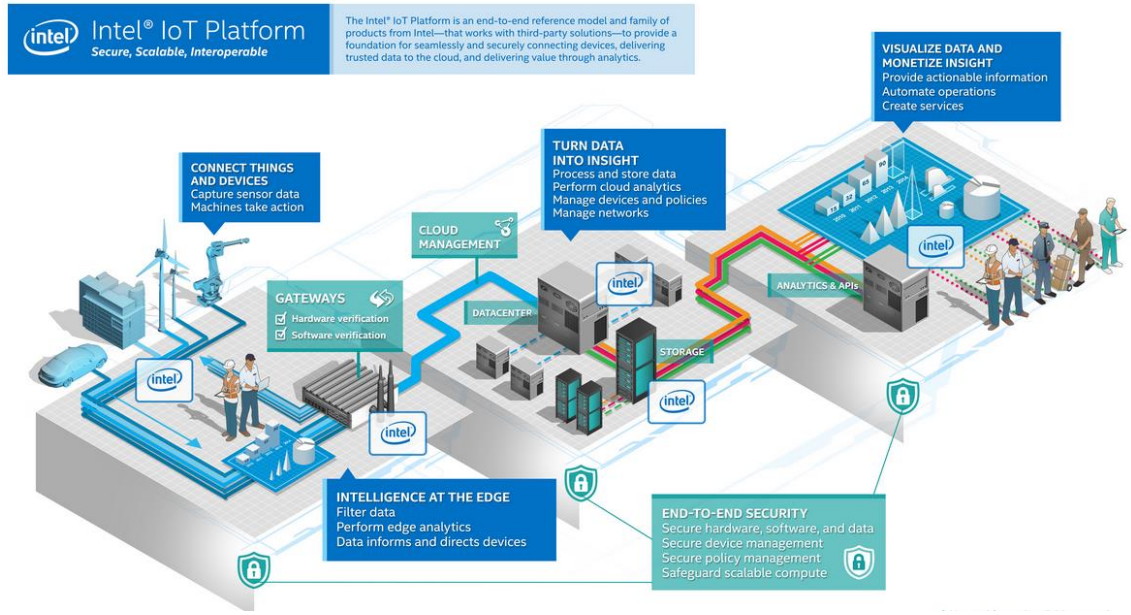


Figure 31 Intel IoT Platform (Intel, 2014a).

Intel is a member of Open Interconnect Consortium with Atmel, Broadcomm, Dell, Samsung and Wind River. This group is targeting to deliver a specification, implementations and certification programs for wireless IoT devices. (Intel, 2014)

5.2.4 Microsoft

Microsoft's IoT solution is Azure IoT suite. Azure is based on cloud technology and it provides a set of functionalities, which aims to expand the customer's IoT device usage. These functionalities are based on asset monitoring and results of this monitoring are processed by Azure for better efficiency, improved performance and revenue stream. (Microsoft, 2015)

Microsoft announced with Toshiba that they will do cooperation to jointly develop IoT solutions. Toshiba's contribution is their IoT devices and sensor-data-driven applications. (Toshiba, 2015)

5.2.5 Cisco

Cisco is promoting its own approach called Cisco IoT. This solution covers six areas, which are network connectivity, fog computing, security, data analytics, man-

agement and automation and finally application enablement platform. All of these areas include a variety of related products and technologies. (Cisco, 2015a) Their offering is focused on helping organizations deploy, accelerate and innovate with IoT (Cisco, 2015b).

5.2.6 Samsung:

According to Samsung in the year 2020 all Samsung's digital appliances are connected (Sohn, 2015). Samsung's IoT commitment steps are shown in Figure 32.

Figure 32 Samsung commitment to IoT (Sohn, 2015).

Samsung announced their new ARTIK platform on May 2015 (Samsung, 2015a). Samsung ARTIK is production ready development platform with three classes of hardware modules. Simplest one is called ARTIK 1 and is aimed to power sensitive devices. ARTIK 1 does not support mass memories as it has only SPI interface, where 4MB of flash are connected as shown on Figure 33.

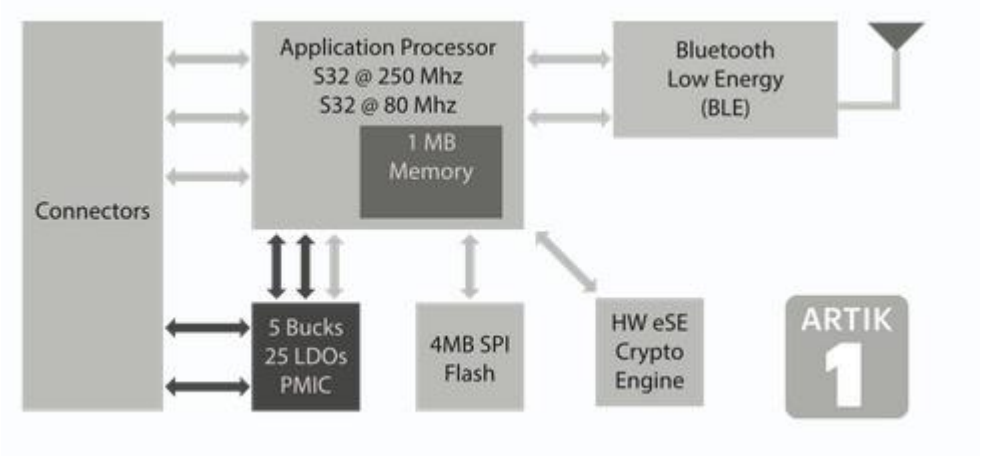


Figure 33 Artik 1 (Samsung, 2015b).

ARTIK 5 is balancing performance and power consumption. As a non-volatile memory ARTIK 5 is using 4GB eMMC in ePOP package. It has a wide set of external interfaces as Figure 34 presents.

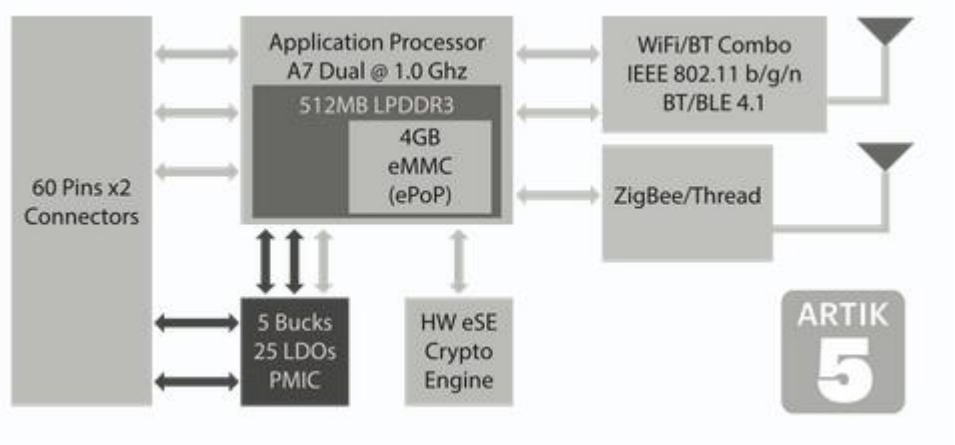


Figure 34 ARTIK 5 (Samsung, 2015c).

The most advanced of ARTIK family is ARTIK 10. ARTIK 10 provides similar performance as Samsung smart phones. (Samsung, 2015d). ARTIK 10 architecture is shown on Figure 35.

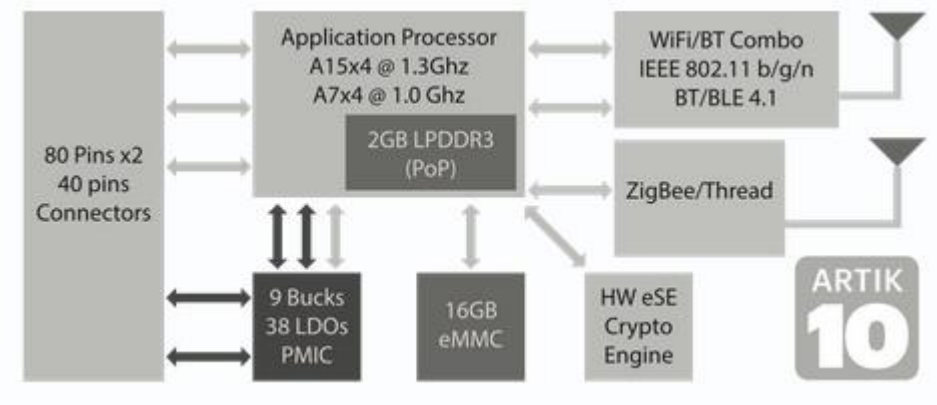


Figure 35 ARTIK 10 (Samsung, 2015d).

For connectivity between devices connected to Internet, Samsung is using Smart Connectivity solution as seen on Figure 36.

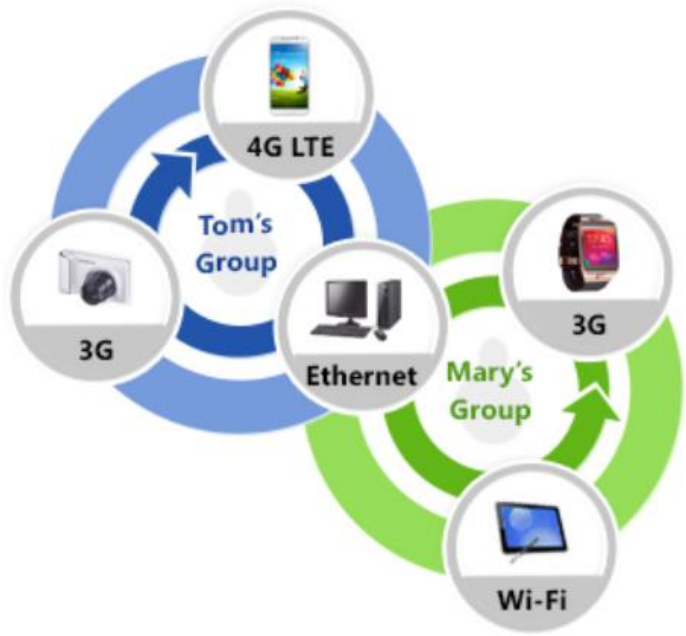


Figure 36 Smart Connectivity solution (Samsung, 2015a).

Samsung sees that IoT has many technical challenges, which are size, power, interoperability, security, insight and ease of development (Sohn, 2015).

5.3 Dependencies and cooperation of IOT forums

As described in earlier chapters there are activities ongoing in multiple forums. Within last year and especially within last two months major industry players have made important announcements. Based on these materials it seems to be that all of the IoT activities are basing their solutions at least partly on the open standards. All of the solutions use Internet as a basic skeleton. In case of local networks players have wide variation from company specific solutions to standardized solutions like WiFi and LWM2M. Security seems to be an area where companies prefer their own solutions. Multiple connectivity protocols are used like Samsung's Smart Connectivity and Google's Weave.

There is important part of companies' activities, which cannot be reviewed from Internet and that is companies' role in the official standard forums. It is extremely likely that bigger companies like Apple, Samsung and Intel have at least a membership in the most of the major forums. However which role they play there is totally unknown. Without that information it is impossible to make estimation if companies plan to implement mainly their own solutions, or they try to modify the official standard to support their plan, or they are just waiting that official standard provides the best solutions. However, based on earlier chapters it is clear that Google and Samsung have decided to make full solutions available with noticeable investments involved to cover missing pieces, which are not defined by official forums.

6. OPPORTUNITIES TO EXTEND AND/OR IMPROVE EXISTING MASS MEMORY USAGE

Key factors for analyzing new use cases were concepts novelty, potential business value, development phase and visibility. The customer company's focus areas are research and development, including related IPRs. Therefore a novelty and development phase are important factors as they define time what company has available for impacting to the end result. For example if solution is already known and technology development is almost done it means there is very little what can be done in order to influence to related standards. The business value of the short term activity might be high, but it includes high risk for the developer of the new technology. In case of long term development it is possible to focus on essential parts of the new trends and therefore reduce the risk of too narrow focus area. Last factor is visibility and that is the reason why selection focuses on local mass memories. There was not enough visibility to mass memory implementations at the cloud so it was not possible to start defining new use cases for those solutions.

One aspect related to the novelty is that all the listed concepts were first drafted as technical solutions. Due to many recent information releases by the companies like Google and Samsung the landscape of known solutions has changed during the last half a year. Therefore some of the aspects or full solutions like advanced testing lacks novelty needed to move forwarded. Still drafting of those solutions was part of the work, therefore all fully drafted solutions are included in the following chapters.

Analyzed use case concepts are organized into two groups. This chapter covers concepts, which are based on existing technologies. Chapter 7 describes concepts, which require a development of new technologies.

6.1 Security peak hole

This use case has developed during the study in a way that original problem statement does not give good support to implementation proposal. Therefore both original and new problem statements are included below.

6.1.1 Original problem statement

Computer security is an important issue to be taken into count by all computer users including the smartphone users. All the computer protections have weak spots (NSA, 2010). The number of people able to take advantage of them is increasing, partly

because of the availability of hacking tools. Therefore it is likely that system connected to the network will have a break in trials if not successful action. News about how governments, criminal organizations and even individuals are breaking in to the computers are common.

The used set of methods is varying from the traditional human factor to advanced high technology methods. The human factor approach can be as simple as sending email with content, which once activated by user will provide access to the computer. Another way to gain from a human factor is to combine it to the technology approach. An example of this is getting access to the computer by luring user to use USB stick with contaminated files or firmware (Lucian, 2014). Also other parts of the computer system like hard drivers can have modified firmware (McAfee Labs, 2015). User might get a virus also by browsing at the internet to the page which is contaminated. Desktop computers have a wide set of security programs, but still certainty of the computer safety is not guaranteed. Mobile devices do not have a similar set of security tools and smart phones are under pressure by criminals now (Srinivas, 2014). Companies like Microsoft, Apple and Google have multiple times been forced to publicly admit that their operating systems have had security issues. Because of concerns listed above, security needs to be layered as shown on Table 2.

Class of Attack	*First Line of Defense*	*Second Line of Defense*
Passive	Link & Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and Personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and Personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

Table 2 Layered security (NSA, 2010).

Still, the result is that user can only do his/her best for the data security, but there is no way to know with high certainty that used methods are enough. The challenge is the uncertainty of both security systems technical level and trustworthiness of the security and/or system providers.

6.1.2 New problem statement

The original problem statement was focused on giving indication if unauthorized access has taken place. During the solution proposal development it was recognized that proposed solution would solve a much wider problem than originally defined. The new problem statement recognizes unauthorized access as a problem, but higher priority is given to the unauthorized changes to the operating system and applications.

6.1.3 Existing solutions

Currently the most common protection approach is to try to prevent a virus from getting control of the system. As a concept, the opportunity to mark files for the surveillance is not new. In case of mobile devices, methods for enabling file level surveillance were not found.

Technology which requires passwords for giving access to locked areas is commonly known and implemented into many mass memories like some of the USB memories, HD drives or memory cards as well as internal solid state memories.

6.1.4 Proposed solution

This solution started from the very simple idea to implement a method how mass memory could trace the access to the predefined part of memory. Activation of this guard function should work also once host unit has a virus. In this case virus should not have an access to the secure logic at the mass memory. These requirements are very difficult to implement in the secure way, once a mass memory interface is the only connection method.

To make the solution clean and secure, an additional host unit and interface are required. This second host would act as a security host and a new interface would connect the mass memory to the security host. One potential candidate to be the second interface is Radio-Frequency Identification (RFID) interface integrated into the managed NAND. Figure 37 illustrates implementation, where managed NAND has RFID as a second interface.

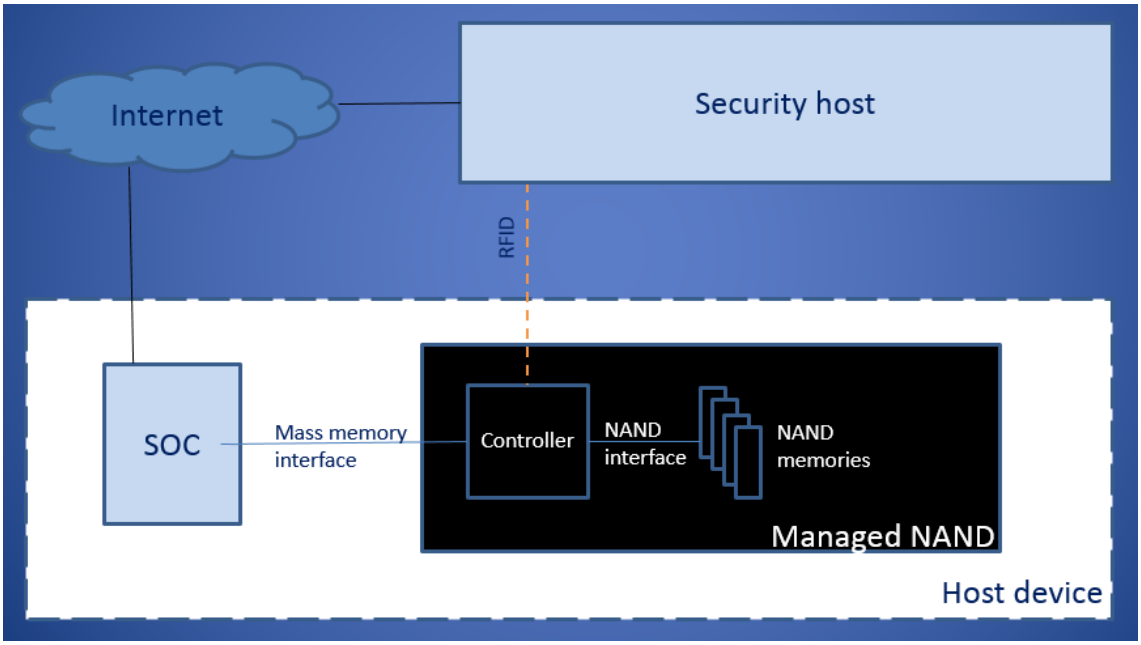


Figure 37 Managed NAND with two interfaces.

However, the good security of this set up requires that security host has higher protection against the threats than the original host. This can be reached either by having better protection software/hardware or by more moderated use patterns at the security host.

RFID interface at managed NAND would be activated via mass memory interface. Communication via both interfaces would include secure identification. In this case it would not be enough for a virus to control the host unit as actual payload communication takes place at RFID interface. Therefore a virus at the host unit could not prevent the usage of the security function without letting user to know about that. Neither would virus be able to make any changes to the secure settings or counters. Secure identification to RFID communication is required so a virus would not be able to activate the RFID interface at mass memory and to use the host's own RFID interface to the secure area. Activation via mass memory interface reduces power consumption and reduces the risk of unwanted scanning. External passive tag can also be included for easier usage. Below the used process steps are defined.

1. The customer buys a new device, which includes default security passwords in RFID interface.
2. A customer changes the passwords
    a. A customer select from the host units menu RFID activation for the managed NAND
    b. A customer selects from the external host unit's menu password update
    c. The external host unit gets old and new passwords from the user input
    d. The external host unit opens a connection to managed NAND with the old RFID password and
    e. The external host unit and managed NAND communicates the password change
3. A customer registers passive RFID tag to the managed NAND by using external host unit

4. A customer defines if RFID requires manual activation or if the interface is continuously active
5. Now security functions have two modes to operate
    a. Automatic, which works once tag is available
    b. Manual, which requires user actions
        i. A user activates with host unit RFID at managed NAND
        ii. The external host unit with RFID password is used to getting access to managed NANDs security functions/settings
        iii. Wanted actions are taken by using external host unit as user interface

In basic implementation, a customer could define that certain file or part of it would be tracked for accesses. Should selected area be accessed a flag would rise. Wear levelling related data access by managed NAND would not rise the flag. The activated flag either causes automatic alarm or is recognized when the system reads status of flag in predefined periods.

An advanced version of the solution enables protection for downloading and locking of the data. During the downloading protection data would be loaded to the mass memory with a normal way. Once downloading is finalized by using the secure communication via RFID interface check sum of the downloaded data could be verified with the original source check sum available from the data provider. With the same method changes in the stored content can be noticed later on.

6.1.5 Novelty, benefits and challenges

As a higher level concept, the idea that visit leaves marks, which are not visible to the visitor is very old. However, the actual implementation is a novelty. The advanced version of the solution includes a novelty also at the concept level

Benefit of the solution is not that it would prevent access to the device, but rather that user would know if unwanted action takes place. Based on predefined action mass memory could then be locked from any access via mass memory interface. Another option is that mass memory would continue to operate, but user would be able to see that somebody has been accessing the secure area.

The main challenge for this concept is convincing the key industry player that they need such solution. Better security is something that is easy to propose, but difficult to provide business benefit. The challenge is that benefit has to be clear for the end customer. Otherwise the interest to invest in additional security is nonexistent. Examples of good technical, but not business wise solutions are multiple security implementation in the mobile mass storage areas. Few of them have provided business benefits.

There are also technical challenges like integrating the RF interface to the managed NAND in a way that it does not disturb either memory or the host functionality and at the same time signal would be available outside the host unit. Antenna implementation would require detailed studies. Considering available technical solutions and the discussion around the RF interfaces, it is possible to solve these challenges with the assumption that length of RF connection is very short.

6.1.6 Cost implications and potential scheduling

If a single interface would be used to implement the proposal, there would not be noticeable cost implications. Dual interface solution would increase managed NAND cost structure. For example access to the peak hole functionality could be done via RF interface from the external devices. In this case optimum solution would be using some existing interface like RFID, which is starting to be widely available at the smart phones. Therefore the only cost addition is from implementing RFID functionality into the mass memory. This RFID access could then be used for some other use cases, for example e-commerce.

In theory, the simplest implementations could be done reasonably quickly if done de facto. In this case, new functionality including the specification work could be available in a year. Should this be a part of the standard then schedule would be about two years. The advanced method would require additional half a year for the de facto approach.

6.2 Advanced testing

6.2.1 Problem statement

Mass memories as any devices have failures during the usage. NAND based mass memories have an extensive set of procedures to handle failures during the operations as it is well known fact that NAND flash has low reliability. However, the main assumption here is that NAND Flash cell is one that fail, but not the used logic. Meanwhile, there is a wide study done by researches of the University of Illinois concerning the failure of the hard drives, which indicates that outages are not always caused by the failure of the media, in this case disk (Jiang et al., 2008). Therefore the problem to be analyzed was how to handle the failure of the logic in case of the mass memory.

6.2.2 Proposed solution and outcome

The built-in self-test (BIST) is a known technology. BIST generates test pattern and then compares the results of the logic. In this new advanced testing managed NAND would have small data block as Read Only Memory (ROM). ROM would include input data for target logic as also expected output data. Either in fixed or by user defined cycles input data from ROM would be fed through for example, the encrypting logic and result would be compared against output data stored to ROM. All this would happen inside the Managed NAND so the target is not to test external functionality but rather to verify working of a certain functional block for example encrypting. Should internal test indicate the error, the managed NAND would inform the host product of test failure. This kind of feature is preferred should the managed NAND encrypt data automatically so user would get early indication that new data will longer be stored in the proper way.

During the concept evaluation, the multiple similar approaches were found. Therefore it was decided that further studies will not be continued.

7. POTENTIALLY NEW IOT USAGE MODELS WITH MEMORY FOCUS

IoT based memory usage models are clearly long term solutions as they require changes to the standards and to the existing devices. However this long term development appears to be promising as can be seen in more details in the following subchapters.

7.1 New type of mass memory

7.1.1 Problem statement

The wish to possess and being able to control often steers the consumer selection. Private network drives and the usage of encryption programs prove of such thinking. Existence of TOR network is also leading to this direction. At the same time there is a high number of user who are not concerned where their data is stored and who has access to that. Cloud drives and applications, running at cloud are evidences of this. In theory cloud drive user could employ an additional encryption program to encrypt stored data, but trust to the service provider's implementation is likely overruling.

Early PCs were not always connected to the network and data was stored to floppy disks or to hard drives. User had full visibility to data. Today's situation is different. A prime example of this are smartphones, which are connected to one or more networks all the time and have numerous data masters like An operating system and applications. Typical smartphone application requires very wide access to the device including stored data. Smartphone user's data copies might be located to cloud and to the local storage. At the end, user has to trust to the device manufacturer and to the operating system as well as to application/s providers that user's privacy is protected and data is not used in the wrong way. In the worst case if this trust is broken user cannot get his data back or copy of the data will stay under control of the service provider. An example of excessive control is Google ecosystem. Google provides the popular ecosystem with a wide range of applications and cloud storage. For user storing his/her own data to this ecosystem means providing reuse rights to Google (Google, 2014). Typically cloud drive user terms grant review rights to the service provider. Some service providers like Apple reserve rights to remove content without request from user. (Patel, 2012) This means that user cannot control what and when will be removed.

Another aspect is who controls the access to user data. If user data is located to the mass storage, which is a part of the system and memory does not have direct con-

nection outside then user does not directly control his/her own data. Freedom to use one's own data is defined by the host device manufacturer and operating system provider. This might mean that even though the host unit is connected to internet user cannot access his/her own data that is inside the host device with another host unit should that be against the interest of the host device or operating system provider. An idea of how changing interest can reduce flexibility/offering is shown in Apple's decision of reduce competition by removing the competing product from the Apple store (Appleinsider, 2015).

7.1.2 Existing solutions

There is a high variety of mass memories. Some of them provide user data control features and some of them are just plain mass memories. A common control feature for local drives is a password for access. In this case, the host unit's user interface is used for the access control settings. A password protected drive can also include automatic encrypting for data. Local mass memory solutions are based on the concept where the local host has full control and therefore it controls the user data.

Mass storage devices with internet access like NAS (Network-Attached Storage) drives provide a wide set of control functions additionally to mass storage functionality. These functions include passwords, but also advanced access controls for example IP based access restrictions are available. In this way, user can define different access rights for different devices. Similarly to the local drives control happens via the same interface, which can be used for mass storage purpose. (Western Digital, 2014)

Cloud drives are used via Internet, but their difference to NAS (Network-Attached Storage) drives is that cloud drives are provided as a service. Therefore typical end user does not know actual implementation. In case of cloud user can setup user level access, but he/she does not have any control to system level accesses. Therefore the service provider has full control of data.

7.1.3 Proposed solution

Bringing back the full ownership of own data to the user can be done by introducing new type of managed NAND. This new memory will provide IoT access to the

mass memory. The key factor for enabling IoT in the local mass memories is change in the mass memory connection. In Chapter 5, the traditional connection type was presented. If the local host uses mass memory as a slave and mass memory does not have any way to pass by the host unit, then mass memory will not be able to operate as an IoT device. This does not mean that host entity could not be IoT device. The way to provide local mass memory access to internet as a master is shown at upper level on Figure 38.

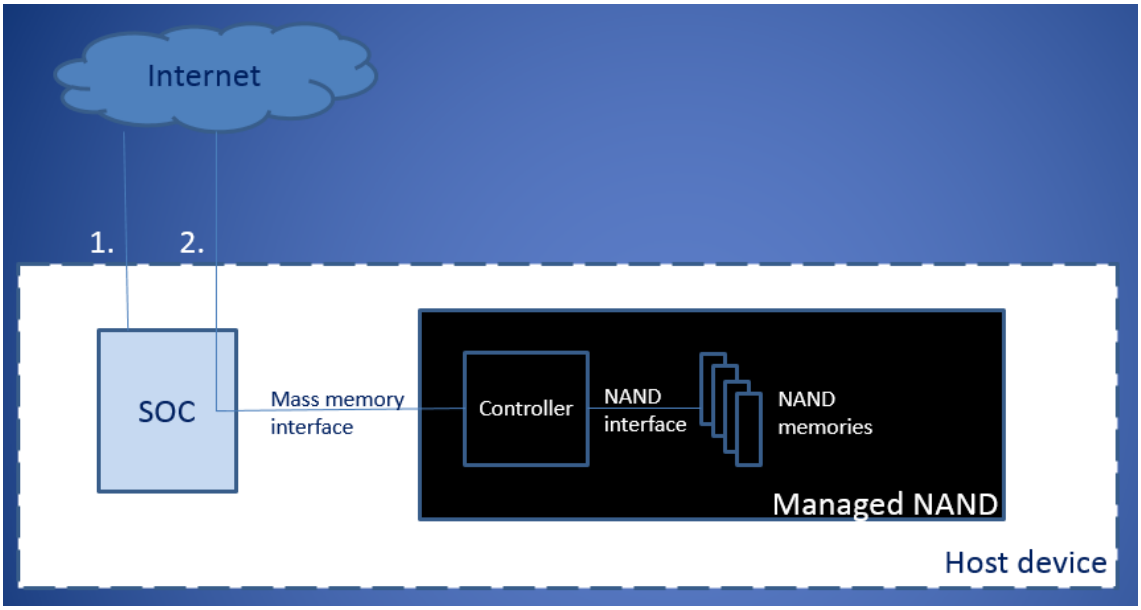


Figure 38 Managed NAND with IoT support.

This kind of managed NAND will further be called IoT NAND. IoT NAND uses system resources for operating power and external data access. Additionally to providing normal local mass memory functions via mass memory interface IOT NAND can operate independently of the host product as a master or a slave to the external devices. In more details, this would be implemented by wrapping Internet protocol to mass memory protocol. The host product would only unwrap mass storage protocol and forward Internet package to external devices. Similarly IoT NAND would receive internet packages from the external device once the process would be done in the opposite order. Figure 39 presents wrapping in case of UFS.

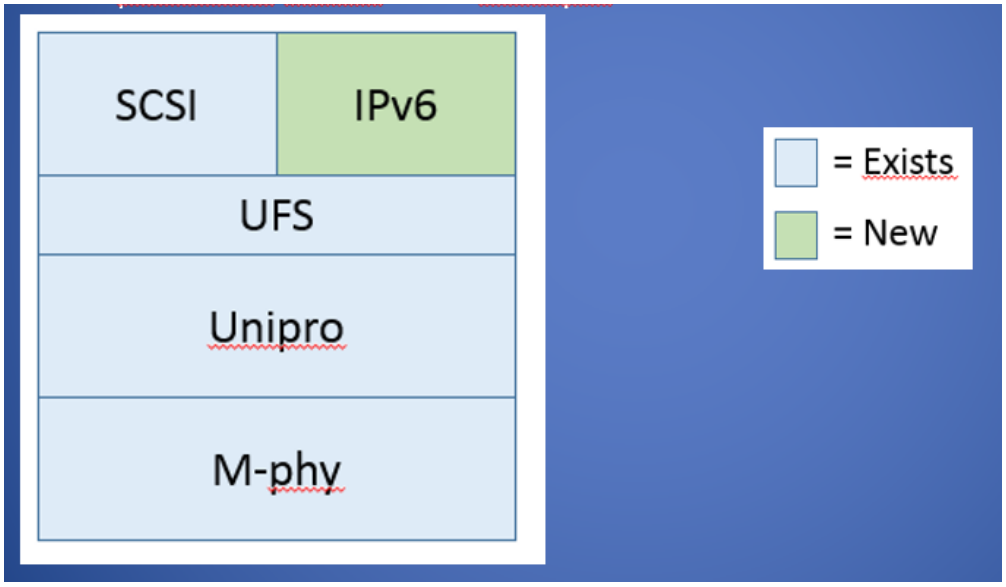


Figure 39 Protocol layers.

In case of lower level IoT devices it might be that they do not support Internet protocol and therefore different protocol package needs to be wrapped as also other communication port is used. One solution would be to use Bluetooth protocol (wrapped in mass memory protocol in communication between host and mass memory) and host units Bluetooth port.

IoT NAND would operate as a master or slave depending of the use case. In the master mode it would collect and potentially process local data. It would also be able to communicate with higher level IoT devices for advanced data processing. Additionally, it could communicate with external devices via Internet for receiving potentially required information. This type of data processing would be a combination of the fog and cloud computing. IoT NAND could also use cloud storages independently of the host unit as well as include means to optionally encrypt data, which would be stored to cloud.

The primary method for the user interface of IoT NAND should be based on IoT type of accessories. Potential delays due to the usage of internet protocol via host device should not be an issue as user interface communication is not time critical in this case. It is also possible to implement an additional RF interface like Bluetooth to IoT NAND for connecting to local accessories, but this would make the host device more complex and would increase the cost of IoT NAND. If devices like displays, speakers and keyboards would be connected as IoT devices the software development work could be done at IoT environment. The option where IoT NAND would share the host unit's resources like the display, speaker and keyboard via communication between IoT NAND and the host unit directly is not recommended. One reason for avoiding is that if the resources of the host device were used then data flowing through them would be under the host unit control and therefore taking away main benefit of IoT NAND. Another aspect is that if the host unit resources are used based on communication between the

host and IoT NAND then host unit has to built-in support for that leading software development to be taking place at both host and IoT NAND environment. In every case, the host needs to have built-in support for wrapping/unwrapping processes defined above for IoT NANDs communication with external devices. In potential future studies it is worth to analyze in more details if the direct connection to shared resources would be justified.

7.1.4 Novelty

IoT NAND is based on managed NAND architecture, which is well known technology. Therefore the combination of the memory technology and the logic is not a novelty. Managed NANDs have independent background operation for example for increasing endurance by doing wear leveling processes in the background. Thus IoT NAND's independent functions are neither a novelty.

Mass storage devices with internet access do exists. Example of such are NAS drives and in the bigger scale cloud drives. Therefore IoT NAND's internet connection is not novelty.

Host devices providing access to mass memory exists. An example of this are all the devices, which provide access to internal mass memory via USB port. However in these implementations host device does not provide independent access as access is rather virtual so the host device is in the control. This kind of implementation could also be considered in order to provide dual access (local/remote), at least at the concept level.

IoT NANDs master/slave functionality is not so clearly known technology. The close one could be small computers, which are connected to TV's HDMI port for upgrading the functionality of the TV. An example device of this kind is Intel Compute (Intel, 2015). A better match is Universal Serial Bus On-The-Go (USB OTG) devices, which uses a single USB interface to operate in both master and slave mode, but used mode needs to be selected for a certain connection (USB Implementers Forum, Inc., 2005). Taken to extreme master mode functionality could take IoT NAND close to the Personal Digital Assistant (PDA)) functionality of the older smartphones where the cellular side was only providing a connection means for the computer side.

As a mass memory IoT NAND is clearly a novelty. IoT NAND concept would allow its functionality to grow independently from the host device. IoT NAND would optionally support a wide range of the access priority, security control and capacity split settings related to IoT and normal local mass memory usage. For example a user could define which part of the IoT NAND is visible to the host unit and which part is visible to the IoT access. The additional novelty is that mass storage would operate independently as master for certain functionalities, which requires communication with devices located outside of the host unit.

The challenging question is if IoT NAND has some functionality what is novelty once IoT NAND is seen as a device, not as a mass memory. So far studies have not shown that there would be a device providing similar dynamical master/slave function-

ality in one interface. Once this master/slave switching is combined with other advanced functionalities of IoT NAND like a mass storage with local and global access it looks that IoT NAND would present a novelty concept.

7.1.5 Benefits

IoT NAND would provide two aspects for the mass memory usage, which are host device driven usage and user defined IoT usage. With proper design memory usages can overlap if user defines so. An example of this would be simple shared memory area for host and IoT usage with proper arbitration procedures. Two use cases enable an easier adoption phase as at the begin IoT could be used in the older product as a plain host driven memory for example to reduce the component portfolio on the host device manufacturer side. This usage would be depending on acceptance of higher cost structure of IoT NAND. Dual support could also allow using IoT NAND in older host designs when older memory design would be ramping down.

As IoT functionality would be separated from the host usage that development could advance independently. The maximum freedom would be reached if the mass storage can be changed by a user. Analysis of existing technical specifications shows that UFS card would provide a good option. Removable IoT NAND would allow user to extend IoT NAND capabilities within the power supply and external interface limits defined by the host unit. This aspect might be tempting for the number of current memory and accessory providers to support IoT NAND. For a user the opportunity to be able to extend functionality can increase the life time of the host unit noticeably.

7.1.6 Challenges

The main challenge of the IoT NAND is not technical. Major challenge would be to convince big host manufacturers to give a control point of user data back to the users. It is unlikely that companies, which are building essential part of their business around the user behavior and data analysis would like to do this. An example of this kind of companies are Google, Apple and Microsoft. In case of a multisector company like Samsung, which has device and memory component business, the resistance might not be so strong. Another aspect is that today economic and technical resource requirements for designing new smartphone are quite low. An example of this is Marshals new smartphone (Svavov, 2015) (Pitkänen, 2015). The low entering cost of the smartphone business could make it possible that even small company, which would focus on the protection of customer data, might make break through. Should one company show with increasing volumes that market exists other would be keener to follow. Apple's entering to smartphone market with touch screen is the prime example of this kind of development.

The cost structure impact on increased performance and functionality is the second challenge. This impact depends on how valuable IoT NAND is made to be to the

customers by the marketing campaigns. If customers see that IoT NAND would provide them with noticeable value cost impact will not slow down the adoption.

Third challenge is the industry reluctance to adopt new solutions. This is the major slow down factor in the area of memories. Many mobile memories like LPDDRs and eMMCs which had been adopted by key manufacturers later on, were adopted much later due to this avoidance of the new solutions. As this item is neither technical nor economic it requires a carefully planned marketing campaign, where the target audience are the decision makers.

Security would be one of the key technical challenges. As IoT NAND is visible at Internet, in the worst case a failure at security would cause so bad a reputation to the IoT NAND that nobody would be willing to implement support for that. Additionally, the concept requires a secure way to move user data from one IoT NAND to the other one for enabling upgrades.

Another technical area, which requires close attention is the architectures of the state machines. As IoT NAND would dynamically switch between the master and the slave modes, it means that likely architecture would have separate state machines for the slave and master modes. Multiplexing between these state machines while sharing the same resources like a mass memory interface to the host requires detailed studies in the implementation phase.

IoT NAND's connection method to accessories provides wide flexibility, but in some cases it makes set up to be complex even if a basic principle is simple. If IoT NAND is located to a smartphone, it cannot communicate with the host unit directly via mass memory interface for the access request to the host unit resources like display and keyboard. Instead, these resources should be available as IoT devices to IoT NAND. Internet protocol introduces challenges to the power consumption as payload is not optimized for low power solutions (Kassner, 2015). Therefore some accessories might need the access to fixed power source, or some power optimized protocol should be used instead of Internet protocol.

7.1.7 Cost implications and potential scheduling

Enabling a host unit to provide needed wrapping/unwrapping with multiplexing is not causing a noticeable cost adder to the host unit design. However, the cost adder to IoT NAND might be noticeable if offered functionality would be more advanced. Basic IoT type mass memory functionality would increase the complexity of mass memory solution, but compared with the cost of NAND memory the cost increase would not be major.

Based on the example of earlier standardization activities, the schedule for IoT NAND is in the range of two years. It consists of one to one and a half year technical work and half a year of approval process at standardization forum. With this schedule, a likely volume ramp up would take place roughly after three years. Essential for the schedule is that two to three major industry players would adopt the concept. Without them, the concept would not likely advance.

7.2 Use case I: Health care application

7.2.1 Problem statement

Population of the elder people in the world is increasing faster than the total population (Geohive, 2015). Therefore it is likely that more people with the need for a medical attention will be living at his/her own home. Essential part of enabling this is to have automated medical surveillance systems supporting living at home. It is not enough to know of the potential medical crises of a patient, but to treat the patient properly medical history is often required. In order to prevent crisis it would be optimum to be able to follow the intake of the medicines and other daily routines like eating and moving. Should elder person leave home it often means that access to patients medical condition nor medical history would not be instantly available. Even if the person would receive instantly medical care in case of crises a proper treatment might not be possible due to lack of medical history.

An increasing number of people use wearable devices mainly for fitness purposes, but at the same time medical information like a heartbeat is available (González, 2015). There are multiple manufacturers providing their own solutions and some of these solutions include data storing in cloud. Data collection for fitness purposes, might sound harmless, but if of detailed medical information is connected with identification information the risk for data abuse later on is increasing.

7.2.2 Existing solutions

The traditional way to connect patient with medical information is a wristband, which includes the ID number used to define some sicknesses directly or by contacting the central database. MedicAlert is an example of using ID number for contacting the central database (MedicAlert foundation, 2015).

Multiple systems where a patient has a wristband or a similar wearable device for collecting medical information were found (Vandrico Inc, 2015). Common for these devices is that they do not have advanced processing capabilities. Both solutions – local only local and local with remote services exist.

7.2.3 Proposed solution with analysis

By using IoT NAND, it is easy to implement a user friendly data collection and a processing method. The safest solution would have IoT NAND in the wristband so it would follow a patient all the time.

IoT NAND would collect person’s local health information and analyze it. Information collection could include a wide range of supporting data from movement sensors, door sensors and others. Based on the analysis results IoT NAND would either

save the data to its secure partition or additionally it could approach external resources for example an emergency support or cloud server for future actions. IoT could also provide local notifications like alarm sounds or it could access some local devices with more advanced user interfaces. This would provide the strong communication method for reminding a user about the important item like the medicine taking. If even simple display is available, the reminder could include a picture to support the message. Similarly if speaker is available an audio message could support the reminder. A user could define external communication, for example select, if an automatic emergency call would be made or data could be stored to a cloud and if the cloud server could be used to extend the analysis. Should the copy of data be stored to a cloud, IoT NAND could automatically encrypt this data. In this case, if cloud service or connection provider had a security leak it would not impact to the security of the data. If the cloud server is doing an advanced data processing, a user could define, which part of the data is readable/writable by the cloud server.

There could be a full ecosystem of the different category devices. The wristband device would enable limited memory density and processing power. Wristband could synchronize its content with the higher class host unit, which would include more advanced IoT NAND with more memory and better processing capabilities. Instead of this, a higher class mobile unit user could have fixed installation were the wristband would communicate with the fixed host unit, which would include IoT NAND with good memory and processing capabilities. User's mobile IoT NANDs could access a fixed one for the data storing or processing power requests even if user would be away from the home. If processing is not time critical, it could also be done in a way that data is collected in the mobile units and later on processed at local IoT NAND. Cloud resources could be used as well.

The concept would require a secure way to move collected data to the new version of the managed NAND as the data collection is supposed to happen over the tens of years. This way user can be certain that his/her data will not be lost as often happens with modern devices once they get old.

Based on the studies a novelty of the proposed system does not lie in the local medical information collection. A novelty consists in the way how this data is processed and stored. Once a customer is at the control of IoT NAND content it is possible to implement customized solutions and be sure that data is available even if the used host unit would cease to exist.

The proper realization of IoT NAND based medical implementation would provide flexible and secure way to collect required information. By processing this data, a patient could receive proper notifications, advice and alerts.

To gain full benefits a wide range of compatible devices like host units and IoT NANDs would need to exist. Similar way, a cloud support should exist for optimum offering. An essential part of the usability is how well applications running at IoT NAND work. For the optimum user interface functionality IoT NAND would require

access to display and speakers, which are IoT type of devices. Availability of these accessories is essential.

A cost structure and potential schedules for this use case are the same as for IoT NAND.

7.3 Use case II: collection of environment data for house

7.3.1 Problem statement

Most modern houses in Finland have the effective insolation, moisture blocking plastics on the walls and the roofs, the automated heating systems and the air conditioner, which operates at both incoming and outgoing air flows and sometime it includes also cooling. Typically the air conditioner includes heat collection functionality. The heating systems include a wide range of optional technologies like the ground and air heat pumps, direct electricity heaters, oil heater. More advanced houses have centralized house automation and multiple sensors for temperature and moisture. Failures in the design, installation maintenance or abuse of the devices can lead to the damages, which might be difficult to notice without opening the structures like the walls or inside roof. (Rantama et al, 2003) An example of such damage is mold caused by excessive moisture. (Sisäilmayhdistys, 2015) Usually, mold damages are difficult to notice at the early phase. Uncertainty of the technical condition of the house makes it difficult to start required maintenances on time, as well as it has a bad impact to the saleability of the house. Therefore a maintenance strategy is required. Figure 40 shows the concept for the maintenance strategy.

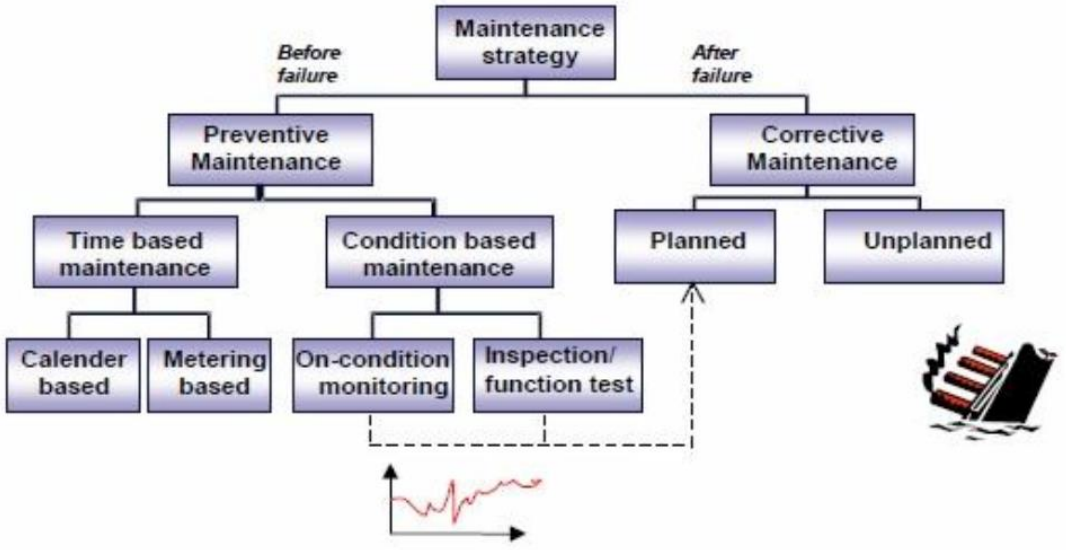


Figure 40 Maintenance strategy. (Mäntylä, 2015)

As Figure 40 shows the failure preparations have two streamlines – taking the action before or after the failure. A good technical solution provides methods of supporting a maintenance strategy in both cases.

7.3.2 Existing solutions

There are house automation systems, which provides possibility for store data from the sensors to local storage. Some of these systems are focused on house automation and some of them are providing house automation as an additional functionality.

7.3.3 Proposed solution with analysis

The optimum situation would be if every house has its environmental log available for later analysis including potential real time warnings for critical changes in the parameters. This kind of house would have set of sensors for environment parameters like heat, air flows and moisture, as well as means for collecting information about essential maintenance operations like air conditioners filter change. In ideal world data collection would be enough, but in real life data trustworthy needs to be guaranteed. This means that sensors with data processing and storage unit have to form a secure entity. As the data content is valuable it would be recommended to have e-commerce level of security implementation including certification for the modules. The system described above could be done by using IoT NAND. In the optimum utilization IoT NAND would be inside the host unit, which would have fixed installation inside the house. IoT NAND would collect data from the sensors in pre-defined intervals. Collected data would then be processed and stored to the IoT NAND. Copy of the data could be transmitted to the cloud storage in the encrypted form. The cloud copy would be valuable in case of the fire or major electrical failure like thunderbolt.

As a higher level concept, the proposed solution does not introduce a novelty implementation. Solution's novelty is at the implementation philosophy. The concept is aiming to have the trust worthy environmental log of house in digital format. Collected data is stored to IoT NAND, which controls the data according to settings defined by user. At the same time, the concept provides an opportunity for the real time warnings of critical failures and reminders for coming maintenance actions.

Trustworthy environmental data collection, processing and storing provide noticeable benefits for the owner of the house. First benefit is real time warnings once the followed parameter is reaching the critical value defined. This could happen when the moisture level inside the house would increase suddenly or over the time. Another example would be the maintenance related timing warnings like reminder to clean the kitchen hood. An example of benefits based on processing of the collected data is advice to start using a out-of-doors setting if the sensors notice that there are longer periods per day once nobody is at home. This would save money and energy due to reduced heating, lightning and ventilation. The new aspect of the data collection is gain from the history log. Selling the house with the trustworthy environmental history log would be

much easier. If the log shows that house has not had water leaks and inside air's moisture and temperature have been within recommended range, it is simple for a buyer of the house to make a decision. The log can also be used for the planning of the future fixing like the heating unit upgrades.

Essential to reach listed benefits is parameters followed and how the following is implemented. It is not enough to have right parameter data if it is not reliable nor reliable data concerning the wrong parameter is useful.

If the data trustworthiness cannot be guaranteed, a key part of the benefits is lost. Even in this case collected data is useful, but it no longer provides proof of the usage history of the house. To gain all the benefits a wide range of compatible devices like host units and IoT NANDs would have to exist. Similar way cloud support should exist for optimum offering. Essential part of the usability is how well applications running at IoT NAND are working. For the optimum user interface functionality IoT NAND would require the access to display and speakers, which are IoT type of devices. Availability of these accessories is essential. IoT NAND would also need to have means to connect with sensors. The connection method could be either some lower level interface like Bluetooth or Internet connection could be used directly.

The cost increase for the new house price is in range of couple thousand euro depending on the amount of sensors and collected data. In the early phase, certificated modules would also have a premium price, but with higher volumes that cost is not expected to be high. The cost increase compared with the house having the centralized automation unit is in the range of hundreds of euro.

Potential schedule for this use case is similar to IoT NAND. Certification availability could bring additional delays.

8. CONCLUSION

Managed NAND architecture is and will be the major part of the NAND business, which will continue to grow. One primary driver for this is uncertainty related to memory technology development. As long as the actual memory array can change dramatically it is safer to use managed NAND architecture, which provides an efficient hiding layer between used memory technology and the host system. Better performance via the managed NAND's separate controller is also a reason to continue using this architecture. As managed NAND architecture will be a major solution there is motivation to seek ways to gain from the existing architecture via introducing advanced non memory related functionalities.

IoT provides means for things with various intelligence to exchange information with each other automatically. The important development trend is increasing amount of data at all the layers of the IoT ecosystem. The proper handling of that data will be essential and could actually define the viability of IoT. Who would accept a connection to the environment where the leakage of the essential data would be probable? IoT ecosystem is forecasted to have strong growth in volumes and its economic impact is estimated to be in the range of trillion US dollars per year over the next ten years on average. It can be said that IoT has already reached the critical mass so the question is no longer if it will be success. The question for the future is what will be the implementation form of the IoT, which will make the break through. These considerations make IoT to be an interesting investment target for the high technology industry as can be seen in the latest industry actions covered at earlier chapters. It seems to be that major industry players are not trying to reach fully compatible solutions except at the higher level like internet protocol. So far the IoT ecosystem has had competing variations in definitions. This is challenging situation for the smaller companies as they need to select between the de facto standards if they want to enter to IoT business now. Situation is also challenging for the whole IoT business as in the worst case competing solutions make the whole sector to be not tempting to the end customers. The smart home development has been an example of bad business due to consumer confusion. Failure in the reducing the number of the competing variations in the ecosystems leads to the risk of not reaching business potential of IoT. Concentrating potential control to one or two companies via IPRs can cause similar end results.

IoT is tempting development area and managed NAND architecture provides a flexible platform to build a wide range of new usage scenarios. Essential part of this development work is to agree about IoT NAND concept. The target should be that mass memory has independent Internet access, which makes it to be a member of IoT family.

Second aspect is that IoT NAND can gain from the managed NAND architecture, which allows the flexible processing power increase on the mass memory side especially if IoT NAND would be implemented in the memory card form factor. Independent Internet access and increased performance enable almost the limitless set of new use cases based on IoT NAND. This thesis has shortly described several early studies of the potential usage concepts. It is important to notice that current host manufacturers might not see reason why mass memory should increase its role at the system. IoT's philosophy to connect everything with everything might change the way how modern systems are built dramatically. Therefore it would be in the best interest of the memory companies and the low end host device manufacturers to develop managed NAND to support IoT. It is likely that there will be similar kind of the power struggling as there was in case of NAND technology selection, but a organization which will want to provide the best in class solutions for the future should have IoT support specified for the mass memory. Once the technically good standard for mass memory with IoT support exists and proper marketing activities are taking place the prospects of the solution are good.

REFERENCES

Aalto University, 2015. *Smart Maintenance.* [Online]
Available at: http://www.aalto.fi/en/midcom-serveattachmentguid-1e513fc6a86640e13fc11e5b2a2ed660804bbc4bbc4/leaflet_aiic_jari_collin.pdf
[Accessed 22 July 2015].

Abraham, M., 2014. *Architectural Considerations for Optimizing SSDs.* Santa Clara, Flash memory Summit.

Ambedded Technology, 2015. *Embedded system for IoT Gateway and Smart Home.* [Online]
Available at: http://www.ambedded.com.tw/pt_list.php?CM_ID=20150326001
[Accessed 25 June 2015].

Appinions, 2014. *Internet of Things Influence Study.* [Online]
Available at: http://dj.appinions.com/iot-july-2014/
[Accessed 9 July 2015].

Apple, 2015. *Introduction to Homekit.* [Online]
Available at: https://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/HomeKitDeveloperGuide/Introduction/Introduction.html
[Accessed 9 July 2015].

Appleinsider, 2015. *Apple removes Nike FuelBand, Jawbone UP from stores ahead of Apple Watch debut.* [Online]
Available at: http://appleinsider.com/articles/15/03/11/apple-removes-nike-fuelband-jawbone-up-from-stores-ahead-of-apple-watch-debut
[Accessed 24 July 2015].

Beecham Research Limited, 2015. *M2M/IoT Sector Map.* [Online]
Available at: http://www.beechamresearch.com/article.aspx?id=4
[Accessed 11 April 2015].

Camhi, J., 2015. *How GE is building the connected city.* [Online]
Available at: http://www.businessinsider.com/how-ge-is-building-the-connected-city-2015-5?IR=T
[Accessed 24 June 2015].

Campolargo, M., 2014. *Internet of Things a policy perspective.* Sophia Antipolis, ETSI.

Cisco, 2015a. *Deploy and Innovate with IoT.* [Online] Available at: http://www.cisco.com/web/solutions/trends/iot/cisco-iot-system.html [Accessed 6 July 2015].

Cisco, 2015b. *Internet of Things (IoT): Portfolio.* [Online] Available at: http://www.cisco.com/web/solutions/trends/iot/portfolio.html [Accessed 9 July 2015].

Cocota, A. & Blodget, H, 2012. *The future of mobile.* [Online] Available at: http://www.businessinsider.com/the-future-of-mobile-deck-2012-3?op=1&IR=T
[Accessed 19 2 2015].

Danova, T., 2014. *THE INTERNET OF EVERYTHING: 2014 [SLIDE DECK]*. [Online] Available at: http://uk.businessinsider.com/the-internet-of-everything-2014-slide-deck-sai-2014-2?op=1?r=US
[Accessed 11 April 2015].

Edson, B., 2015. *Creating the Internet of Your Things.* [Online] Available at: https://www.microsoft.com/en-us/server-cloud/internet-of-things.aspx#Fragment_Scenario1
[Accessed 6 July 2015].

Elliot, J. & Brennan, B., 2014. *Industry Innovation with Samsung's Next Generation V-NAND.* [Online] Available at: http://www.flashmemorysummit.com/English/Collaterals/Proceedings/2014/20140805_Keynote2_Samsung.pdf
[Accessed 18th April 2015].

ETSI, 2014. *BRAINSTORMING: IOT@ HOME.* Sophia antipolis, ETSI.

European Research Cluster on the internet of things, 2015. *Internet of Things.* [Online] Available at: http://www.internet-of-things-research.eu/about_iot.htm [Accessed 11 4 2015].

Floman, M., 2012. *Mobile Memories.* Santa Clara, Jedec.

Geohive, 2015. *Population pyramids: World.* [Online] Available at: http://www.geohive.com/earth/world_age.aspx [Accessed 23 July 2015].

González, Z., 2015. *The New Smart Wristbands for 2015.* [Online] Available at: http://www.wearable-technologies.com/2015/02/the-news-smart-wristbands-for-2015/
[Accessed 23 July 2015].

Google, 2014. *Google Terms of Service.* [Online] Available at: https://www.google.com/intl/en/policies/terms/
[Accessed 22 July 2015].

Google, 2015a. *Google Cloud Platform: Solutions.* [Online] Available at: https://cloud.google.com/solutions/
[Accessed 6 July 2015].

Google, 2015b. *Why Google Cloud Platform.* [Online] Available at: https://cloud.google.com/why-google/
[Accessed 6 July 2015].

Handy, J., 2014. *What's Changing In NAND Flash and What Isn't.* Santa Clara, Flash Memory Summit.

HUTGRIP, 2015. *Market opportunity for the next "big thing".* [Online] Available at: http://hutgrip.com/blogs/market-opportunity-for-the-next-big-thing/
[Accessed 25 June 2015].

IDC, 2013. *Where in the world is storage.* [Online] Available at: http://www.idc.com/downloads/where_is_storage_infographic_243338.pdf
[Accessed 9 July 2015].

IEEE, 2015. *IEEE--SA Internet of Things (IoT) Ecosystem Study,* New York: IEEE.

IERC, 2014. *IERC – Standardization Challenges.* Sophia Antipolis, ETSI.

Intel, 2014a. *Intel® IoT Platform infographic.* [Online] Available at: http://www.intel.com/content/www/us/en/internet-of-things/infographics/iot-platform-infographic.html
[Accessed 9 July 2015].

Intel, 2014. *Industry Leaders to Establish Open Interconnect Consortium to Advance Interoperability for Internet of Things.* [Online] Available at: http://newsroom.intel.com/community/intel_newsroom/blog/2014/07/07/industry-leaders-to-establish-open-interconnect-consortium-to-advance-interoperability-for-internet-of-things
[Accessed 9 July 2015].

Intel, 2015. *Introducing the Intel Compute Stick.* [Online]
Available at: http://www.intel.com/content/www/us/en/compute-stick/intel-compute-stick.html
[Accessed 24 July 2015].

Jiang et al., 2008. *Are Disks the Dominant Contributor for Storage Failures?.* [Online]
Available at: http://opera.ucsd.edu/paper/tos08.pdf
[Accessed 26 July 2015].

Kassner, M., 2015. *Sensors powered by energy harvesting key to IoT success - See more at: http://www.electronicsweekly.com/news/internet-of-things/sensors-powered-by-energy-harvesting-key-to-iot-success-2015-08/#sthash.cxiKHN1M.dpuf.* [Online]
Available at: http://www.electronicsweekly.com/news/internet-of-things/sensors-powered-by-energy-harvesting-key-to-iot-success-2015-08/
[Accessed 14 August 2015].

Kilbuck, K., 2014. *Is 3D NAND a Disruptive Technology for Flash Storage.* Santa Clara , Flash memory summit.

Klas et al, 2014. *"Lightweight M2M": Enabling devices management and applications for the Internet of Things.* [Online]
Available at: http://openmobilealliance.org/about-oma/work-program/m2m-enablers/
[Accessed 7 July 2015].

LoRa Alliance, 2015. *LoRa™ Technology.* [Online]
Available at: http://www.lora-alliance.org/What-Is-LoRa/Technology
[Accessed 11 June 2015].

Lucian, C., 2014. *Most USB thumb drives can be reprogrammed to silently infect computers.* [Online]
Available at: http://www.pcworld.com/article/2460540/most-usb-thumb-drives-can-be-reprogrammed-to-silently-infect-computers.html
[Accessed 23 July 2015].

MarketResearch.Asia Group, 2014. *DRAM, China, and Leading-Edge Foundry Driving IC Industry in 2014.* [Online]
Available at: http://www.marketresearch.asia/dram-china-and-leading-edge-foundry-driving-ic-industry-in-2014.html
[Accessed 9 July 2015].

McAfee Labs, 2015. *McAfee Labs Threats Report: May 2015.* [Online]
Available at: http://www.mcafee.com/us/security-awareness/articles/mcafee-labs-threats-report-may-2015.aspx
[Accessed 23 July 2015].

McGarry, G., 2015. *Macworld: The first 5 HomeKit accessories are finally here.* [Online]
Available at: http://www.macworld.com/article/2929751/the-first-5-homekit-accessories-are-finally-here.html
[Accessed 9 July 2015].

Mcguirk, D., 2015. *SEMI Equipment and Materials Outlook.* Seoul, SEMICON Korea.

MedicAlert foundation, 2015. *MedicAlert foundation.* [Online]
Available at: http://www.medicalert.org/
[Accessed 25 July 2015].

Mehraban, S., 2014. *IoT North America: Embracing the Internet of Things Today.* [Online]
Available at: http://blogs.intel.com/iot/files/2014/05/IoT-NA-Shahram-Prez.jpg
[Accessed 12 April 2015].

Micron, 2006. *Technical Note, NAND Flash 101: An Introduction to NAND Flash and HowtoDesignItIntoYourNextProduct.* [Online]
Available at: http://www.ece.umd.edu/~blj/CS-590.26/micron-tn2919.pdf
[Accessed 23 May 2014].

Micron, 2013. *NOR | NAND Flash Guide.* [Online]
Available at: www.micron.com/ -/ media/ Documents/ Products/ Product%20Flyer/ NOR_NAND_Flash_Guide_lo.pdf
[Accessed 24 May 2014].

Microsoft, 2015. *Microsoft Azure IoT services: Learn more abouit the Azure IoT service.* [Online]
Available at: https://www.microsoft.com/en-us/server-cloud/internet-of-things.aspx#AzureIoT
[Accessed 9 July 2015].

Mylly, K., 2015. Tampere: s.n.

Noronha, A., Moriarty, R., O'Connell, K. & Villa, N., 2014. *Attaining IoT Value: How To Move from Connecting Things to Capturing Insights.* [Online]
Available at: http://www.cisco.com/web/solutions/trends/iot/docs/iot-data-analytics-white-paper.PDF
[Accessed 18 May 2015].

NSA, 2010. *Defense In Depth.* [Online]
Available at: https://www.nsa.gov/ia/_files/support/defenseindepth.pdf
[Accessed 23 July 2015].

Patel, N., 2012. *Is Google Drive worse for privacy than iCloud, Skydrive, and Dropbox?*. [Online]
Available at: http://www.theverge.com/2012/4/25/2973849/google-drive-terms-privacy-data-skydrive-dropbox-icloud
[Accessed 22 July 2015].

Pattison, S., 2014. *IoT, Silos, Solutions and More.* Sophia Antipolis, ETSI.

Pichai, S., 2015. *IO: keynote.* [Online]
Available at: https://events.google.com/io2015/videos
[Accessed 6 July 2015].

Pitkänen, P., 2015. *Kuuluisan kaiutinmerkin uutuuspuhelin suunniteltiin Suomessa.* [Online]
Available at: http://www.itviikko.fi/teknologia/2015/07/23/kuuluisan-kaiutinmerkin-uutuuspuhelin-suunniteltiin-suomessa/20159348/7
[Accessed 24 July 2015].

Rannou, H., 2014. *Innovation in Internet of Things: questions and challenges about standardization -The point of view of a startup.* Sophina Antapolis, ETSI.

Rantama et al, 2003. *Terve talo -teknologiaohjelma 1998 - 2002.* [Online]
Available at: http://www.tekes.fi/globalassets/julkaisut/terve_talo.pdf
[Accessed 22 July 2015].

Samsung, 2015a. *Samsung Announces ARTIK Platform to Accelerate Internet of Things Development.* [Online]
Available at: https://www.artik.io/media#press-releases
[Accessed 7 July 2015].

Samsung, 2015a. *What Is Smart Connectivity Solution?*. [Online]
Available at: http://developer.samsung.com/smart-connectivity
[Accessed 7 July 2015].

Samsung, 2015b. *Hardware ARTIK1*. [Online]
Available at: https://www.artik.io/hardware/artik-1
[Accessed 9 July 2015].

Samsung, 2015c. *Hardware ARTIK5.* [Online]
Available at: https://www.artik.io/hardware/artik-5
[Accessed 9 July 2015].

Samsung, 2015d. *Hardware ARTIK10.* [Online]
Available at: https://www.artik.io/hardware/artik-10
[Accessed 9 July 2015].

SD group and SD card association, 2013. *SD Specifications Part 1Physical Simplified* , San Ramo: SD card association.

Sisäilmayhdistys, 2015. *Homevaurioiden ehkäisy ja tunnistaminen.* [Online] Available at: http://www.sisailmayhdistys.fi/paasivuista-toinen/homevaurioiden-ehkaisy-ja-tunnistaminen/
[Accessed 22 July 2015].

Sohn, Y., 2015. *Unleashing a Bold Era of IoT Innovation.* [Online] Available at: http://iotworldevent.com/keynote-presentations/unleashing-a-bold-era-of-iot-innovation/
[Accessed 6 July 2015].

Srinivas, 2014. *Android Hacking and Security, Part 1: Exploiting and Securing Application Components.* [Online] Available at: http://resources.infosecinstitute.com/android-hacking-security-part-1-exploiting-securing-application-components/
[Accessed 23 July 2015].

Svavov, V., 2015. *The Marshall smartphone is a cynical branding exercise done right.* [Online]
Available at: http://www.theverge.com/2015/7/17/8987697/marshall-london-smartphone-android-design
[Accessed 24 July 2015].

Tal, A., 2003. *Two Technologies Compared: NOR vs. NAND.*. [Online] Available at: http://maltiel-consulting.com/Nonvolatile_Memory_NOR_vs_NAND.pdf
[Accessed 5 May 2014].

Toshiba, 2006. *Toshiba NAND vs. NOR Flash Memory Technology Overview*. [Online] Available at: http://umcs.maine.edu/~cmeadow/courses/cos335/Toshiba%20NAND_vs_NOR_Flash_Memory_Technology_Overviewt.pdf
[Accessed 11 April 2015].

Toshiba, 2014a. *e•MMC.* [Online] Available at: http://www.toshiba-components.com/memory/emmc.html
[Accessed 26 May 2014].

Toshiba, 2014b. *MLC NAND.* [Online] Available at: http://www.toshiba-components.com/memory/mlc.html
[Accessed 26 May 2014].

Toshiba, 2015. *NAND Interface: SmartNAND™*. [Online] Available at: http://toshiba.semicon-storage.com/eu/product/memory/nand-flash/mlc-nand/smartnand.html
[Accessed 19 June 2015].

Toshiba, 2015. *Toshiba Builds Partnership with Microsoft to Deliver New Internet of Things (IoT) Solutions.* [Online] Available at: https://www.toshiba.co.jp/about/press/2015_06/pr0301.htm
[Accessed 7 July 2015].

Tsai, V., 2010. *e·MMC v4.41 and v4.5 Architecture for High Speed.* [Online] Available at: http://www.jedec.org/sites/default/files/Victor_Tsai.pdf
[Accessed 25 5 2014].

UFSA, 2015. *UFSA.* [Online] Available at: http://universalflash.org/
[Accessed 22 June 2015].

Umbrellium, 2015. *Thingful.* [Online] Available at: https://thingful.net/
[Accessed 2 July 2015].

USB Implementers Forum, Inc., 2005. *Introduction to USB On-The-Go.* [Online] Available at: http://www.usb.org/developers/onthego/USB_OTG_Intro.pdf
[Accessed 24 July 2015].

Vandrico Inc, 2015. *Sproutling Baby Monitor.* [Online] Available at: http://vandrico.com/wearables/device/sproutling-baby-monitor
[Accessed 25 July 2015].

Vermesan, O. F. P., 2014. *Internet of the Things - From Research and Innovation to arket Deployment.* ISBN: 978-87-93102-95-8 ed. s.l.:River publishers.

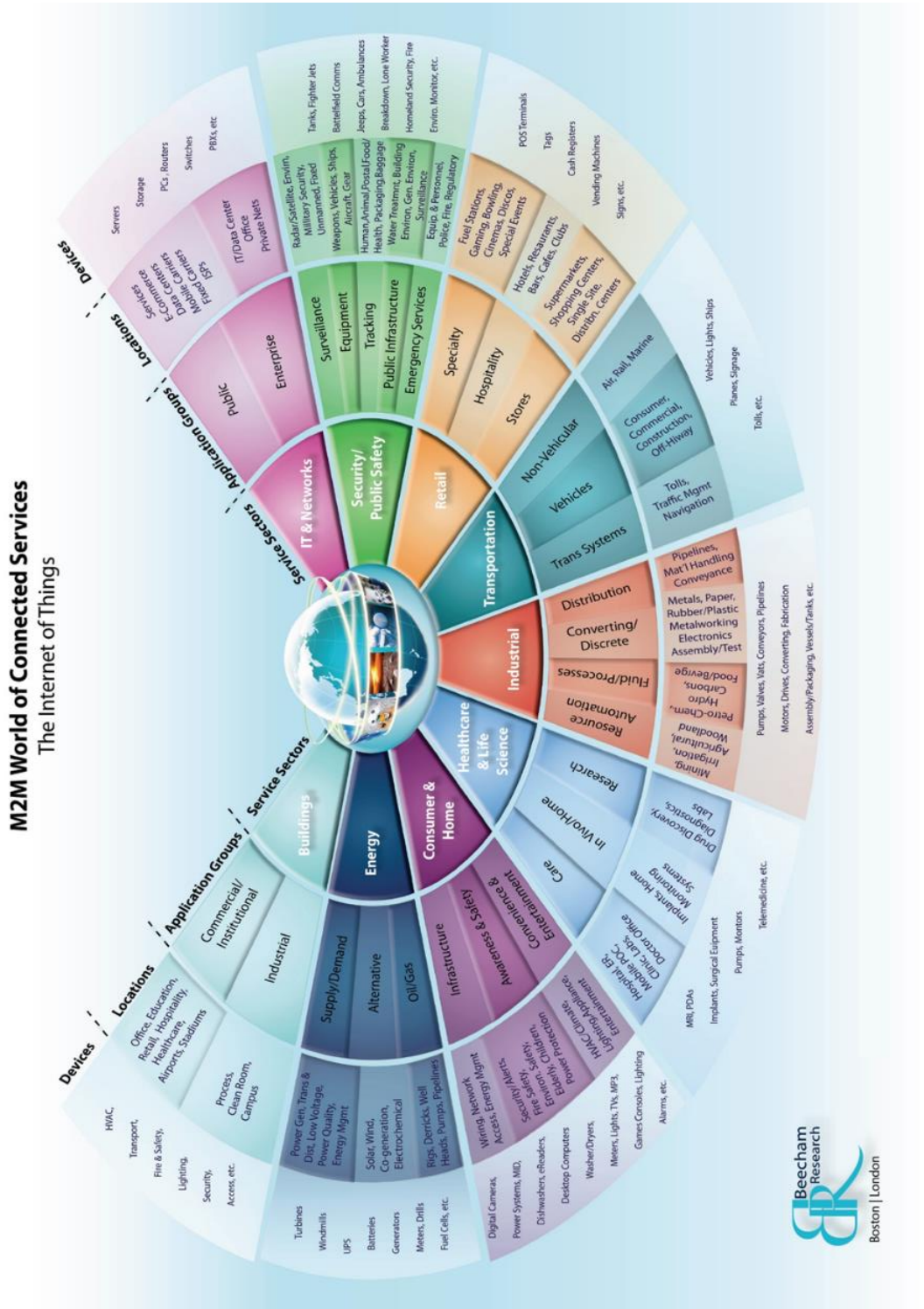
Western Digital, 2014. *WD My Cloud EX2, Personal Cloud Storage, WD My Cloud EX2.* [Online] Available at: http://www.wdc.com/wdproducts/library/UM/ENG/4779-705119.pdf
[Accessed 13 August 2015].

Wirepas, 2015. *Technology behind multi-hop mesh IoT platform.* [Online] Available at: http://www.wirepas.com/technology/
[Accessed 25 June 2015].

Wirepas, 2015. *Wirepas PINO.* [Online] Available at: http://www.wirepas.com/Pino_Product_Brief.pdf
[Accessed 24 June 2015].

Wood, N., 2015. *Ericsson in U-turn over 50bn connected devices prediction.* [Online] Available at: http://www.totaltele.com/view.aspx?ID=490158 [Accessed 24 June 2015].

APPENDIX



Attachment 1 Internet of Things use cases (Beecham Research Limited, 2015)