v. 1.4

TASSTA

WHITEPAPER / 2022

CHOOSING THE RIGHT MOBILE DEVICE

For your organization's
PTT solution

CONTACT

TASSTA GmbH
Bödekerstrasse 56
30161 Hannover
Germany

TASSTA Inc.
300 Sevilla Ave Ste 205, Coral Gables, FL 33134,
USA

TASSTA Technologies FZE
DSO-THUB-G-D-FLEX-G118
Dubai Silicon Oasis, Dubai

www.tassta.com
mail@tassta.com
+49 511 727520-21
+49 511 370170-29 (FAX)

WHO SHOULD READ THIS?

- IT Directors, Managers and Support
- Network and System Administrators
- Operations Improvement Managers
- Dispatch Managers
- Communications and Distributions Managers
- Enterprise Mobility Managers
- Mobile Device Managers
- Procurement, Technology
- Innovation, Operations, or Customer Support departments within an organization that have a high demand for instant one- to-one or one-to-many voice communication to improve productivity in the workforce.
- Carrier agents especially PTT Specialists, Account Managers and Sales Managers.

WHICH INDUSTRIES CAN BENEFIT?

- Agriculture/Farming
- Airlines
- Building Materials & Equipment
- Business Services
- Casinos
- Construction
- Defense
- Education (K-12, Higher-Ed)
- Government
- Healthcare
- Hospitality
- Law Enforcement
- Manufacturing
- Mining
- Oil & Gas
- Public Safety
- Retail
- School Districts
- Security
- Transportation & Logistics
- Utilities
- Waste Management
- Wholesale

EXECUTIVE OVERVIEW

You have identified your two-way radio communication strategy as part of your digital transformation project and now you're thinking, "Where should I start?" Since your PTT over LTE solution is most likely a smaller project within a larger digital transformation project, it's important to consider which components are required for multiple digital transformation projects and which components are exclusively for the PTT over LTE project.

As mentioned in our whitepaper, How to Realize the Benefits of Digital Transformation in Your Organization's Two-Way Radio Communication Strategy, a PTT over LTE solution requires:

MOBILE DEVICES

The mobile phone will most likely be the centerpiece of your digital transformation project as it often has several roles.

Data Collection: Data is either automatically collected without the involvement of the end user such as GPS data, a connection to other devices (such as IoT devices in manufacturing or ELD in a truck) or it is directly entered by the end user through a user interface (UI) which can be a screen, keyboard, scanner, reader and camera among others. The data collection component is usually made possible through an application.

Data Transmission: Data in all forms is being sent and received almost continuously, in which the mobile phone acts as a transmitting device together with the data network.

DATA NETWORK

The data network is very closely linked to the mobile phone providing the channel to transmit data. In most cases it will be an LTE network but could also be a local WIFI network which would have its own requirements. In both cases, the data network extends across the entire digital transformation project and is not exclusive to the PTT over LTE project.

PTT APPLICATIONS

The PTT application if not integrated into a bigger solution can be seen as solely part of the PTT over LTE project.

PTT ACCESSORIES

The PTT accessory will in most cases work specifically with the PTT application although there are cases where programmable buttons can give commands to other applications to simplify repetitive work processes (such as setting a waypoint on a GPS application).

PITFALLS TO SELECTING MOBILE DEVICES

Since the mobile phone and the data network might be crucial to several digital projects, this whitepaper will provide tips on how to choose the best mobile device and pitfalls to avoid. Just because the mobile device is critical to the PTT over LTE solution, it does not mean that the process is linear. You cannot choose your mobile device without understanding which PTT applications and accessories it's compatible with and will best serve your organization.

When the topic of buying mobile devices comes up, the first person we think of is the carrier agent or even better, the mobility service provider and these are generally the right people to go to for advice. Nevertheless, a common pitfall is that often the discussion will focus around the cheapest price with the latest offers as well as the number of subscriptions and how big of a data package is required. However, your carrier's agent should also be able to understand the requirements you have for the device and offer a portfolio of their solutions and those belonging to other third-parties that align to the needs of your digital transformation project. If the agent cannot do that, consult other providers with expertise such as the potential PTT application or accessory providers as they have a customer base with similar objectives and challenges as yours.

The second pitfall is around mobile phone brands. Brands make us feel attached to certain values that we attribute to them and we might have had a good or bad experience with certain brands in our pasts which skew our decision making.

This is one reason why we see differences in market share across regions. While in North-America, Samsung had a market share of 32% in Q1-2017 followed by Apple with 22%, their global market share was significantly less with Samsung at 23% and Apple at 15%1 and while Huawei holds a global rank #3 with 10% market share, their leading success in their native country of China, does not translate to the US market (<1%)2. This is a perfect example of why it's crucial to collect all requirements across markets/regions and then neutrally evaluate to find the best solution.

COLLECTING REQUIREMENTS

When collecting the requirements for the PTT over LTE project, different perspectives need to be considered:

1. THE USER'S PERSPECTIVE

This perspective will help to identify the appropriate hardware form factor and the level of ruggedness the device should have. Requirements should answer the following questions:

- What data needs to be collected?
- How will it be collected?
- What data needs to be accessed?
- Is there any legislation/laws that need to be considered?
- What is the work environment?
- What is the skillset of the workforce?
- Will the user directly communicate through the mobile device or will it be through an accessory? *Specific to the PTT over LTE project.

2. THE SYSTEM'S PERSPECTIVE

This perspective will help to identify what capabilities the mobile device needs to have. The system's perspective covers technical requirements through answering the following questions:

- How will the mobile device communicate with the system?
- What is the lifecycle of the device?
- What are compatibility requirements for applications and accessories?
- What are the security requirements?
- How much budget is available?

IDENTIFYING REQUIREMENTS

FROM THE USER'S PERSPECTIVE

In Identifying the requirements from the user's perspective, the first theme is around data and how it will be collected or accessed.

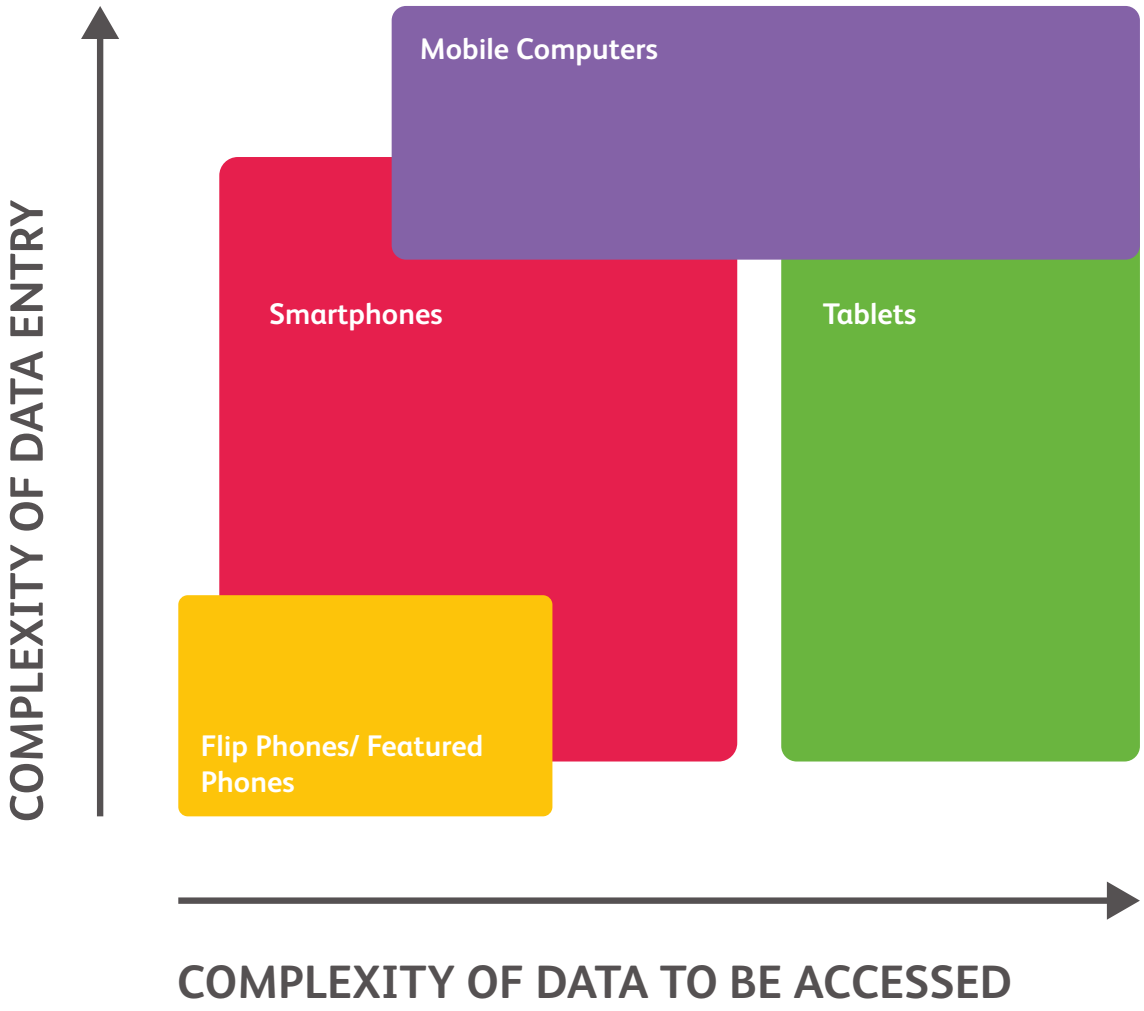
DATA COLLECTION AND ACCESSIBILITY

There is almost a correlation between the complexity of the data and the size of the device. If data needs to be entered in a more manual way, the bigger the

device will be. And, in the same way, the more complex the data that needs to be entered or accessed is, the bigger the device will be.

Some Examples:

- Collection of GPS data is achieved automatically by almost any type of mobile device, without any data entry required. Nevertheless, if GPS data needs to be accessed, a bigger screen like that of a tablet to display map features is an advantage compared to a regular smartphone.
- For basic voice communication via PTT over LTE, smaller devices such as simple feature phones, smartphones, or even iPods could be sufficient as the only requirement is a button on a screen needing to be pressed as well as audio needing to be recorded or played.
- Most mobile devices are built with cameras that can be used for capturing simple data, like taking pictures or even scanning bar codes.
- For more manual data entry or capturing signatures, a bigger screen or even a keyboard may be required which is available on mobile computers.
- The access of highly complex data like CAD drawings or blueprints requires not only sufficient processor capacity, found on larger devices, but also a more suitable interface like a keyboard or mouse to navigate.


Mobile Computers
Smartphones
Tablets
Flip Phones/ Featured Phones
COMPLEXITY OF DATA ENTRY
COMPLEXITY OF DATA TO BE ACCESSED

QUICK OVERVIEW OF THE DIFFERENT FORM FACTORS OF MOBILE DEVICES

Feature phones and flip phones had their success mainly due to lower costs, a certain level of ruggedness, radio-like look and simple functionality that made it easy for a less technology savvy workforce to use the device purely for PTT communication without specific training. For a long time, flip phones have been the most sold form factor by carrier reps thanks to incentives and low price points but the decline of these type of phones has been steep with a 7.9% decline in feature phones over the year 2016 while smartphone sales grew 2.5%. The primary reason is that these phones often use proprietary OS firmware.

Since the market size is so small most application vendors do not make the effort to implement their app with platforms like Java or BREW. The capacity and software of these phones is significantly inferior to those of smartphones and data entry and access is also very limited.

SMARTPHONES

Smartphones are the ideal tool for most applications including PTT over LTE solutions. Using a standard operating system (OS) like Android or iOS, they allow a wide range of integrations to all kinds of applications that allow automatized as well as manual data entry supported by standard features such as touchscreen displays, sensors, GPS, NFC, high resolution cameras, and microphones.

TABLETS

Tablets are like smartphones with a larger screen size (>7 inches/18 cm) which is a trade-off at the expense of wearability and compactness. Apart from the bigger battery which has only slight improvements on total usage time; as the screen requires more power, there are no real improvements on CPU or memory compared to a smartphone. The main advantage is that the larger screen allows better accessibility of data and is especially useful for GPS and map usage. That's why we see tablets being used within in-vehicle applications such as trucks, busses, and taxis. It is very important to notice that tablets are still considered mobile phones and the use behind a steering wheel is against distracted driving regulations unless an accessory is used with it such as a speaker mic which allows one button touch communication functionality.

PORTABLE MEDIA PLAYERS

Portable Media Players run standard operating systems and can therefore load any type of applications; even PTT applications. They are significantly cheaper than smartphones and do not require a subscription which does limit their use to a defined perimeter which can be covered by a solid WiFi network. There are other downsides to these devices as they are not designed for use cases other than media applications. Another problem is that most of these players go into sleep mode if not used for a certain period of time.

MOBILE COMPUTERS

Mobile computers are significantly more expensive than mobile phones and offer a more tailored feature set from a hardware and software perspective for specific use cases. The most recognized examples of mobile computers are bar code scanners as well as label printers used in warehouse management, logistics, and retail applications.

PTT PHONES

Tailored for PTT over LTE usage, there is a specific category of phones called PTT phones. What makes them different from regular consumer phones is that they are equipped with a dedicated PTT button on the side of the device to facilitate PTT communication. PTT applications would map the PTT function to the side button to allow PTT communication without having to unlock the screen or phone, something that is usually only bypassed by PTT accessories. These PTT phones are often more ruggedized than the consumer phone as they are intended to be used in outdoor work environments.

LIMITATIONS WITH DATA COLLECTION

Depending on the country of residence of the end user and the organization, there are a few limitations with data collection. Since it is an employee using the device, there are certain rules involved on what data can be collected and what cannot. Some of them, depending on the country have been made into laws by legislators, others are imposed by work councils or labor unions.

For example, the continuous tracking of GPS data (even in taxis) might not be possible in some countries or needs to be approved by the work council or labor unions.

Another new legislation is the General Data Protection Regulation (GDPR) created by the European Union which will was enforced on May 28, 2018. The GDPR impacts all companies with employees living in EU countries. GDPR sets ground rules on how to handle personal data not only for end customers in B2C businesses but also for employees in B2B organizations with potential penalties of up to 4% of the total worldwide annual turnover of the preceding financial year. Before a major digital transformation project in Europe, this regulation should be reviewed with legal council as the implications are high.

WORK ENVIRONMENT

The next component of the requirements analysis should be about the type of work environment that the mobile device will be taken into, which will determine the ruggedness of the device. Most of these requirements align with certain standards that phones are tested against.

RUGGEDNESS

There are different criteria to look for depending on the work environment. Some ruggedness testing is standardized with IP ratings or MIL-STD 810G while others are manufacturer defined.

DROP TEST

Since phones get dropped so regularly, most manufacturers have tested their phones against drops from different heights (usually 1.5m up to 2m), even for consumer devices.

DUST AND WATER

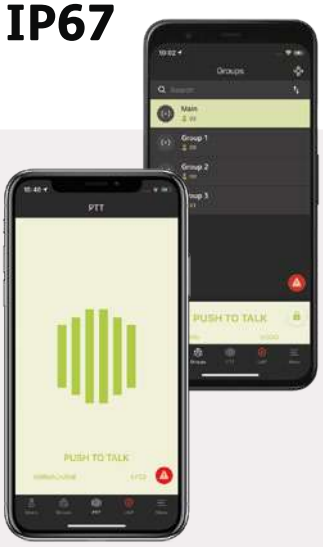
How dirty and wet the environment can be, are covered under the Ingress Protection (IP) standards. The IP number is composed of two numbers, the first referring to the protection against solid objects and the second against liquids. The higher the number, the better the protection.

First Number	Second Number
0 - No protection (Sometimes X)	0 - No protection (Sometimes X)
1 - Protected against solid objects > 50mm	1 - Protected against dripping water (~1mm / minute)
2 - Protected against solid objects > 12.5mm	2 - Protection against dripping water when tilted at 15°
3 - Protected against solid objects > 2.5mm	3 - Protection against direct sprays of water up to 60°
4 - Protected against solid objects > 1mm	4 - Protection against water splashed from all directions
5 - Dust protected	5 - Protected against low pressure jets of water
6 - Dust tight	6 - Protected against powerful jets of water
	7 - Protected against temporary immersion (<1m for 30min)
	8 - Protected against longer immersion at higher pressure (as defined by manufacturer)

PITFALLS ON CONSUMER DEVICES

While many think that "consumer" devices are completely different from "professional" devices, in terms of IP ratings, the difference is very small. Most "consumer" devices nowadays already have at least an IP67 rating:

IP67



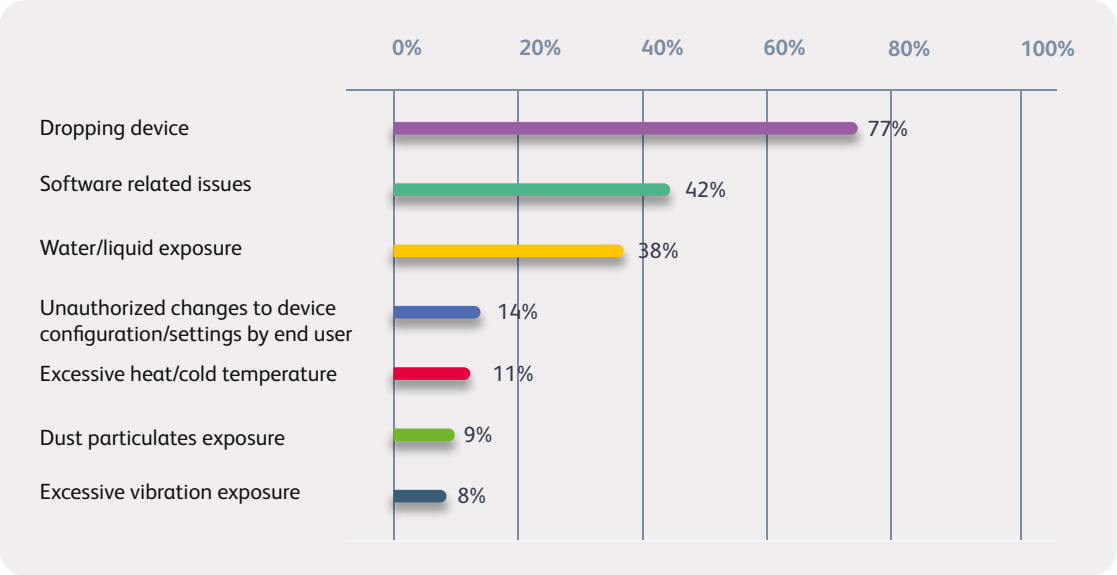
iPhone, Google Pixel
2 – 3.2 feet (1m) for 30 min

IP68

Samsung Galaxy XCover FieldPro
6.5 feet (2 m) for 30 min
*Ruggedized phone manufacturer

SAMSUNG

LEADING CAUSES OF DEVICE FAILURE



Source: VDC Research Group Inc. (2013)

MIL-STD TEST SPECIFICATIONS

500.5	Low pressure (Altitude): especially if the devices are produced overseas and transported via an aircraft
501.5	High Temperature: in hot and humid regions or even for in-vehicle use during summer
502.5	Low temperature: for use in cold regions
503.5	Temperature Shock (defined as temperature change greater than 10°C (18 F): for indoor and outdoor use
504.1	Fluids: such as diesel, gasoline, oils, disinfectants and cleaning fluids, fire extinguishants
507.5	Humidity: depending on the region
509.5	Salt fog: for use on ships
514.6	Vibration: for use in vehicles
516.6	Shock: basically, a drop test for the device itself or during shipping6
Sensors	Accelerometer (only for Man Down and Detect Impact feature)
Battery / Charger	Battery capacity 1700mAh or more USB charging

TEMPERATURE

Temperature, both high and low as well as temperature changes, can be a challenge to any device. As mentioned, standardized testing has been established by the Department of Defense (DOD) in the MIL-STD-810G test method standard within tests 501.5, 502.5 and 503.5. Pitfalls around the operation of mobile devices in extreme temperatures (which can occur in vehicles in summer or winter) are:

- High temperatures starting at around 60°C or 140 F, cause the device to go into slow mode or even switch off completely. The device will only switch back on when it has securely cooled down. High temperatures may also damage the battery.
- Low temperatures especially below freezing have a significant impact on the battery life and also on the charging behavior.

EXTREME PRESSURE & PUNCTURES

Especially for big screen devices, such as smartphones and tablets, the weak point is usually the screen. Rugged mobile device manufacturers have developed testing against extreme pressure and punctures to provide appropriate protection against cracking of the screen.

WARRANTY

Even if you have chosen a device which fully matches your environmental requirements, it will not protect it 100% from breaking. If you have chosen a device that meets your requirements and it fails nevertheless, due to a manufacturer defect, you want to make sure that you can return it, even after the standard one year manufacturer's warranty to get a replacement or your money back.

INTRINSIC SAFETY

Intrinsic safety (IS) is a protection technique for safe operation of electrical equipment in hazardous areas by limiting the energy, electrical and thermal, available for ignition. Intrinsic Safety (IS) devices can be used in explosive environments without the risk of igniting combustible elements. IS approved phones are commonly used in industries like mining or oil and gas. High-risk environments like this are subcategorized in classes and divisions for the US approvals for IS. ATEX/Ex regulations are used in the European Union.8 The specific approval received for a particular phone will determine in which zones it can be used. When using the phone with a wired accessory, the approval for intrinsic safety must be done together in order to be valid. The phone doesn't automatically receive IS approval even if it's being used in conjunction with an IS approved accessory. Unless it is a Bluetooth accessory, an IS approved mobile phone and a separately approved accessory together, do not constitute an IS approved solution.

BATTERY LIFE

If the mobile device is assigned to one single worker who works eight hours, any mobile device would probably do the job. If used for two or three shift cycles by multiple workers, the battery life needs to be tested. This is also required for the charging behavior. How often can the device be charged and for how long? Will this time be sufficient to last for the next shift? Something to consider is also how and where the mobile devices will be charged and the logistics involved around the charging process.

Examples:

- How and where will 100 workers charge their mobile devices?
- Will the truck driver take the mobile device out of the truck or will he leave it in the cabin?

The best way to verify if a device battery life is sufficient for your needs is to run a proof-of- concept pilot for two to four weeks with a small group of end users. Do not trust specifications from the mobile phone manufacturer as the battery life varies depending on multiple factors.

SAFETY ATTIRE

Your workers will very likely wear some kind of work clothes. Will these uniforms impact the use of a mobile device?

Gloves:
Standard gloves prevent the user from using a smartphone as swiping or typing is not possible. They also limit the tactile ability to locate buttons quickly.

Hearing protection:
Hearing protection not only protects the ears, it may also prevent the user from hearing the phone.

Protective suits:
Will the user be able to access the phone? Can it actually be worn outside of the suit or will it need to be worn within it?

Use of the above safety attire is a good indicator that either a specialized PTT phone or PTT accessory will be required.

WORKER SAFETY

Are your workers operating in potentially dangerous environments? If the answer is yes, you will need to provide some options to protect them. Currently there are two available solutions; one which is active and the other, which is passive.

The active solution is a mobile device with an emergency button. This button, once pressed, can trigger an alert or warning that something is not right to an operator. The functionality of the button is often application dependent and not an automatic feature of the phone, however the phone would allow this feature to be easily triggered through a specific button. Use cases could be in public safety, security, or even housekeeping in hospitality where personnel could get into potentially dangerous situations.

The passive alternative requires the phone to be able to measure acceleration as well as balancing of the phone which most of today's smart phones do facilitate. Again, in combination with an application, these phone features can help identify if the user fell or is laying on the ground or hasn't been moving for the last five minutes and inform an operator automatically.

BRAND REPUTATION

An often-neglected criteria for choosing a solution is reputation. This is especially valuable for industries that are scrutinized for their brand image and ability to deliver optimal customer service, such as hospitality, retail and healthcare institutions. For example, if staff using PTT over LTE technology are in direct contact with customers and the solution isn't stable or reliable, customer service could be compromised and therefore brand reputation could be at risk. In addition, having staff use old technology devices instead of the latest iPhone for example may not align with the high-end, luxury brand image your organization may be trying to portray.

IDENTIFYING REQUIREMENTS FROM THE SYSTEM'S PERSPECTIVE

Within this part of the requirement analysis of the mobile device, we do not look at how the user will utilize the device but rather at the requirements that concern the people that have to manage the devices and integration in the overall system. These can be different roles within the IT team such as IT asset managers, mobile device managers, network administrators but can also be simply the managers of the workers themselves such as fleet managers. It is important to consider the whole lifecycle management of the device and the costs and resources required to move the device through the life cycle.

DEVICE MODEL

You might run across a carrier sales representative that has a compelling special offer on an older or carrier specific mobile device at a lower price. Looking at the complete lifecycle of the device and considering a failure and loss rate (warranty case or not) of 5-10% every year, what if you want to buy another 50 of these devices? Will they still be available or will you have to buy completely different devices? Will these older devices still be upgradable to keep up with the newer ones? This can turn into a very difficult support scenario where you will be maintaining a multitude of different devices over the years with different operating systems and software which makes troubleshooting and upkeep, very resource intensive. It's crucial that the cost of the device be evaluated against the lifecycle maintenance costs of the system.

OPERATING SYSTEM (OS)

The options here are Android or iOS and both have advocates that support the OS specific pros. In short, iOS is a proprietary software and therefore easily controllable by its owner, Apple which has a curated app store and provides a higher level of security. On the downside, there are more limitations for customization in this wall-gardened ecosystem.

Android on the other hand is an open source software that can be easily customized and even in-house applications can be easily created. The selection of phones is significantly higher with a bigger price spread across devices. Nevertheless, due to its open platform it is also more prone to malware and because not every Android version is exactly the same, the patching and updating can be troublesome on devices that do not follow the standard.

UPGRADABILITY

Don't opt for old devices that run on old iOS or Android which won't be upgradeable in the near future. As apps develop further for new OS versions, an old OS on the phone might lead to significant issues which are not worth the hassle.

EXOTIC OPERATING SYSTEMS AND WALL-GARDENED ECOSYSTEMS

Yes, there are other OS systems out there aside from Android or iOS, including Java or BREW. Some other manufacturers want to keep their systems completely closed to not allow any other systems to mess with their software or hardware. The selection of mobile devices with non- standard software should be carefully evaluated. Unless there are capable programmers available in-house that can work on specific platforms to develop custom apps, an integration to other systems might be very costly. If the device is solely used for a specific single purpose without interactions with other systems, this could still be a possible solution.

SOFTWARE & HARDWARE COMPATIBILITY

The likely reason why you are buying the mobile device is to run specific applications on them that drive better data and productivity around the whole value chain of the company. It's probably already on your radar to ensure that the PTT application of your choosing is compatible with the device, however compatibility goes beyond the OS version number. Does the device support the required data upload and download speed of the application? What is the storage capacity of the applications or can the processor of the device handle the multitude of all the apps that are supposed to run simultaneously? Are background applications (MDM software, tracking apps, antivirus, encryption) able to work on the device?

SECURITY

Mobile device security is a complex topic and you should consult with your IT security or mobile device management (MDM) team about it. Several considerations should be discussed which may impact your mobile device lifecycle management strategy.

- **Theft**: It's no surprise that tablets and smartphones are in high demand with workers. Disgruntled employees often feel like they need to get more out of their former employer and it's not uncommon that a tablet or phone disappears. Some employees find a second source of income stealing and selling company property. Third party theft is of course possible, too. A PIN allows for blocking any unauthorized user from using a stolen device but impacts the ease-of-use of a device by the authorized user. There are companies that have reported loss rates of around 15% not including broken devices. It is therefore important for a company to be able to track and trace the devices; a solution that houses an inventory of the devices and who owns it and can trace the devices© whereabouts. Many PTT applications support geolocation to follow and record the route a user has been taking. But a system should also be able to withstand a factory reset that deletes all installed applications so that a stolen and wiped device can be traced back to the delinquent. Apple provides good solutions to track devices via iCloud. Samsung has Knox which also can survive a factory reset. A third solution is Absolute, a company that provides a persistent piece of software enabled through code embedded into the BIOS of over a billion devices.
- **Malware**: This is a smaller problem if the device is locked and can only be used by specific applications that only access specific internal data sources. Such white-labeled applications can be controlled by mobile device management (MDM) or Enterprise Mobility Management (EMM) solutions which also facilitate the deployment and configuration of such applications to the whole device population. Leaders in this segment are: VMware Airwatch, MobileIron, IBM and BlackBerry.9 Should a device also use an email account and have access to a mobile browser and the user is free to download and install any application or software, the device is prone to cyber attacks. Should the device have access to more data than that in a demilitarized zone (DMZ) the company data is at risk. Devices can maintain a good security posture if they have an up- to-date OS and applications. Some companies have adopted a bring-your-own-device (BYOD) policy where employees can use their own devices if they subscribe to the security requirements of the company. This saves costs but also often mixes business and private data if not properly separated.
- **Data**: Storing any sensitive data like customer, pricing or employee data on the device's hard disk drive, should be avoided. Through theft or cyber attacks, this data could get into the hands of the wrong people which can sabotage a company's reputation and even lead to compliance breaches and fines. Are you thinking about device life-cycle management? Are you planning to sell the devices after a certain time period? How can you get all sensitive data off the devices? A simple factory reset may appear to delete all data but there is technology out there that does have the capability of resurrecting this once deleted data.

COSTS

Hard Costs

1. Hardware

- Mobile Platforms
- Peripherals

2. Software
- Upfront Fees
- License Fees
- Development Costs

3. System Design & Integration
- Application Design & Development
- System Integration
- Staging

Soft Costs

1. Training

- Initial User Training
- On-going User Training

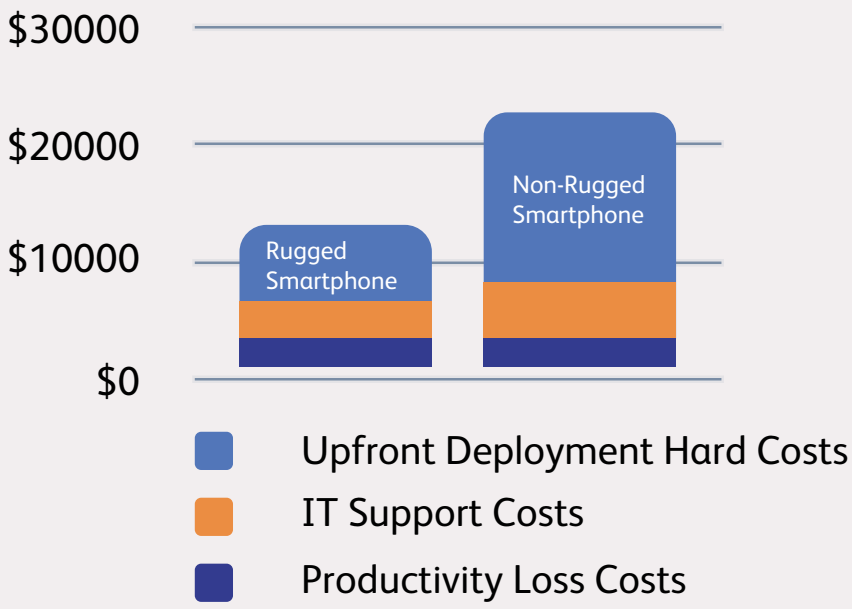
2. Operational
- System Maintenance
- Third-Party Technical Support
- Internal Technical Support
- Upgrades
- Application Management

3. Downtime
- Lost Manpower/ Wages
- Lost Revenues
- HW Replacement

Source: VDC Research Group Inc. (2013)

Most researches such as the VDC study suggest that the TCO of a ruggedized mobile device is significantly lower.For a consumer mobile smartphone, the post-purchase costs are 92% of the complete five year TCO. Although the VDC study is outdated and newer studies are not available or not independent enough, there is a reason why consumer device manufacturers have merged into the ruggedized space as there is a business case for it. So instead of consumerization which is defined as companies adopting technologies that originate in the consumer space, the manufacturers of consumer devices drive a ruggedization to improve the TCO business case compared to ruggedized devices that will increase their market share of the enterprise graded IT solution market.

FIVE YEAR SMARTPHONE TCO



Source: MBC Research Group Inc. (2013)

www.aina-wireless.com

CONCLUSION

The mobile device is the connecting technology between your overall digital transformation project and the PTT over LTE project. When choosing the right mobile device for your organization both the user as well as the system's perspective need to be considered. Questions to ask, include:

- How will data on the device be entered, processed or read?
  – This would define the form factor.
- What does the work environment look like?
  – This would define the specifications for ruggedness.
- How can a company limit the effort required to install, maintain and terminate a whole device population over its lifecycle thus reducing the total cost of ownership (TCO)?
  – This would define software requirements.

Identifying the right mobile device might be the most complex task as it directly needs to meet the requirements of all potential applications and accessories that would be used with the device.

SOURCE

Daniel Hackl, Director Global Sales & Marketing at AINA Wireless

Daniel Hackl has provided consulting to hundreds of customers in small and large companies and organizations across all industries during their PTT over LTE projects. Over his career he has established an extensive network of partners within the PTT over LTE ecosystem that he leverages to find the right solution for his clients.

Daniel Hackl holds two Masters degrees in business and a certificate in Digital Strategy from the University of British Columbia. He also brings experience in project management and is CompTIA Security+ certified.

Contact Daniel at daniel.hackl@aina-wireless.com or schedule a free consultation.

REFERENCES

1. IDC. Worldwide Quarterly Mobile Phone Tracker. 2017.
2. Fortune. Why Huawei's Chinese Dominance May Not Translate into American Success. 2016.
3. Intersoft Consulting. General Data Protection Regulation.
4. Kyocera Mobile. kyoceramobile.com/business/duraforce-pro/.
5. Samsung. https://tassta.com/samsung/.
6. Department of Defense. Test Method Standard for Environmental Engineering Considerations and Laboratory Tests. 2008.
7. American Communication Systems, Inc. Intrinsic Safety Approvals for Radio Communications Equipment. 2012.
8. European Commission. Equipment for Potentially Explosive Atmospheres (ATEX). 2014.
9. Gartner. Magic Quadrant for Enterprise Mobility Management Suites. 2017.
10. VDC Research Group, Inc. Mobile Device TCO Models for Line of Business Solutions. 2017.

TASSTA

Become your best self.

www.tassta.com, mail@tassta.com

CONTACT

TASSTA GmbH
Bödekerstrasse 56
30161 Hannover
Germany

TASSTA Inc.
300 Sevilla Ave Ste 205,
Coral Gables, FL 33134,
USA

TASSTA Technologies FZE
DSO-THUB-G-D-FLEX-G118
Dubai Silicon Oasis, Dubai
United Arab Emirates

www.tassta.com
mail@tassta.com
+49 511 727520-21
+49 511 370170-29 (FAX)