Dedicated Operating System for AIDC?

Automatic identification and data capture (AIDC) and the technologies surrounding it have become commonplace on warehouse floors and in supply chains throughout the world. From convenience stores to major supermarkets or from global shipping centers to your local post office, chances are you've seen a handheld device that can instantly scan and share information through phone lines or through a wireless connection.

When thinking about the operating systems behind these devices, one might come to a conclusion that a single operating system would dominate the installed population. The reality is that there are three major variants that are in use in the AIDC space:

Legacy Operating System — A platform that continues to be used in spite of its obsolescence and incompatibility with modern equivalents.

Mobile Device Operating System — A mobile device OS generally built to support functions (keyboards, email, text messaging, etc.) and features commonly available on mobile consumer devices.

Dedicated Handheld Operating System — A operating system specifically developed to support functions necessary for AIDC use (retail floor, warehouses, manufacturing, etc.).

At CipherLab, we frequently help companies upgrade their legacy AIDC system to either dedicated or mobile device based systems, giving us a broad and unique perspective on the inherent tradeoffs involved. This paper details points that set these operating systems apart and certain advantages that lead many manufacturers, retailers and suppliers to choose a handheld manufacturer's dedicated operating system.

Lower Costs

For the most part, dedicated handheld manufacturers are focused on producing AIDC capable devices that offer value in specific applications by enabling the requisite hardware capabilities to perform the desired function whether that is enabling the scanner to capture and store the data encoded in a barcode or reliably transfer collected information to a host device. As a result, the proprietary operating systems typically don't require licensing fees as the OS enables the device to function.

This may not be the case with software companies that are developing multiple operating systems that are being adapted to work in the AIDC environment. Since their operating systems are their product, these developers are in the business of generating revenue across multiple platforms ranging from desktops to smartphones. As an "adapted solution" the adapted operating system contains features that have no relevant value in an AIDC related application and the purchaser pays for functions that are not ever utilized. With this scenario, there is a fee and it frequently is based on unnecessary capabilities.

Dedicated handheld operating systems are developed to enable the required capabilities of the hardware platform. Generic mobile device operating systems can be used for a wide array of activities thus customers pay for more functionality even if they don't use it.

When considering the legacy operating system, limitations are frequently reflected by the inability of the old platform to address current business needs. The lost opportunity of savings or advantages of providing current and relevant solutions to business needs often are outweighed by the cost savings available by subscribing to a current solution (ie. the cost of inaction is greater than the cost of change).

Stability and Ruggedness

Most mobile phone operating systems aren't developed for a specific device but generally for a class of devices with common functionality. As a result, they have to be adapted to provide the functionality necessary in an AIDC application. To enable this, drivers have to be downloaded and made to gracefully coexist in an environment not specifically designed for such change. Typically this creates an environment that doesn't compare with the stability offered by dedicated handheld operating systems.

After implementation, another challenge is often created whenever the mobile device operating system is updated or refreshed. Frequently, the "bolted on" AIDC drivers are incompatible with the new update. Users of these types of systems are often subjected to unpredictable results which negatively impact business operations by lost data or corrupted files.

Dedicated handheld operating systems are a different story. Since the manufacturers design the OS specifically for their hardware platform, the OS works in perfect unison with the hardware. These systems can be counted on to operate as designed and offer predictable business use in the intended application.

Devices based on legacy operating systems have reached the maturity that their electronics have degraded to the point that their intended operations just simply aren't reliable. Users of these types of devices are experiencing more frequent repair cycles and starting to realize the need for upgrade. Another concern with legacy operating systems is that AIDC specific devices are finding productive use in areas not imagined when the legacy devices were first released. They just simply don't offer the functionality necessary for deployment in some of these environments.

Higher Level Of Security

A common trend in the utilization of mobile devices is the concern over security from cyber attack or the introduction of malicious viruses into the user community. At a consumer device level, the loss is personal. At the commercial level, these events cost real dollars through the time invested by highly skilled individuals to "clean" the corporate system, getting users back to normal operations and potential data integrity loss resulting in business decisions being made on incomplete or corrupt data.

It is commonly reported that the persons behind these types of activities are motivated to cause the most harm to the greatest audience. As the mobile device operating system based devices include consumer grade offerings, cyber criminals are much more likely to attack systems based on these operating systems. An additional contributing element is that the code and structure of these offerings are much more in the public domain and therefore more accessible when compared to the dedicated handheld operating systems. There is simply much more exposure for the mobile device operating system.

The construction of the dedicated handheld and legacy operating systems is such that the "code" is written to specific functionality of the components of the device and enabling the functions necessary to support the intended application – data collection. As a result, each manufacturer effectively has a "closed loop" system which supports their particular devices and isn't available in the public domain.

Longevity

If one takes the time to observe the various AIDC business applications and the utilizations of application specific or dedicated handheld operating system devices, it becomes apparent that these devices are very prevalent in current business operations. A testament to the longevity of

these devices is the very large population of these units that have been in service in excess of fifteen years (Telxon 610/710, MSI 1475, etc.).

The dedicated handheld operating systems of these devices have continued to offer the functionality designed into these devices and support the business needs of their owners. Only when business needs have exceeded original design (ie. data retention beyond original memory constraints, 2D barcode scanning, etc.) has change become necessary.

Quite the contrast is the experience of devices based on a mobile device operating system. As these are typically developed in the consumer space (Cell Phone and Personal Digital Assistant) and modified to offer the necessary AIDC functions, they are in an environment of a very short lifecycle. Most industry analysts acknowledge that the expected lifecycle of the technology in this market space has now reached six (6) months. Developers making the "bolt on" changes necessary for AIDC function with these offerings must continue to stay abreast of these fast paced changes and adapt to the constraints of the newest generations. The adaption to a new generation could mean an installed base "refresh" to maintain functionality. This hardly seems advantageous in a business atmosphere and has the potential to burden the user base with updates on a frequent basis.

Custom Application Development

As the elements of the OS in a dedicated operating system are those that are essential to the operation of the device (very little, if any, unnecessary overhead), the software developer typically has much less to contend with during the development effort. This results in quicker and, potentially, much less costly application development.

In the mobile operating system environment, the compilers have some degree of inaccuracy and necessitate minute "tuning" to achieve the desired results. In an environment that faces change in a very short time period, this process becomes quite burdensome and tends to drive the cost of development beyond expectations.

When considering software changes or development of enhancements in the legacy device class, the unique challenge is identifying competent and affordable resources to undertake the desired change. Proficiency in the applicable language required simply isn't available or has become scarce so as to demand very high rates for development.

From the discussion points illustrated in the content of this document, it becomes apparent that "proprietary" or dedicated operating systems and the associated hardware platforms have a valid place in the realm of solutions offering AIDC functionality and in some instances may offer unique advantages. For those organizations considering a change in their approach to their AIDC deployed applications, it certainly seems prudent to evaluate this class of solutions.

About CipherLab

CipherLab is a global leader in the design, manufacture, and marketing of Automatic Identification and Data Capture/Collection products and systems. The company's mobile computers and scanners are integrated into the networks of some of the world's best known logistics, retail, distribution, government installations and healthcare companies, helping them run more efficiently and effectively onsite and on the road. CipherLab USA is headquartered in Plano, TX. For more information, please visit www.cipherlab.com.

CipherLab USA, Inc.
2552 Summit Ave. STE 400
Plano, Texas 75074
Phone: 469-241-9779
Email: NASales@cipherlab.com