AUTOMATIC IDENTIFICATION AND DATA CAPTURE (AIDC) AND ITS TECHNOLOGIES

Anto Ramya. S. I

Assistant Professor, Department of Computer Science,
St. Joseph's College of Arts and Science for Women, Hosur, Tamil Nadu, (India)

ABSTRACT

"AIDC refers to the methods of automatically identifying objects, collecting data about them, and entering that data directly into computer systems (i.e., without human involvement)" – Wikipedia. The rise of computers in business made AIDC technologies essential. Automatic identification and data capture (AIDC) is the use of technology to provide direct data entry to a computer, or other micro-processor controlled system, without resorting to manual methods of data-entry. AIDC technologies eliminate two error-prone and time-consuming activities: manual data collection and data entry. AIDC bypasses these two steps by providing a quick, accurate, and cost-effective way to collect and enter data. The alternative to AIDC is manual data collection and retention; this suffers from higher rates of error, greater requirements on time and higher labour costs than AIDC. AIDC technologies provide a reliable means not only to identify but also to track items. It is possible to encode a wide range of information, from basic item or person identification to comprehensive details about the item or person e.g. item description, size, weight, colour, etc. This paper presents an overview on AIDC infrastructure and its various technologies of AIDC with their limitations. Each technology is best suited based on circumstances and cost.

Keywords: AIDC, bar codes, data capture, data collection, RFID.

I. INTRODUCTION

Automatic Identification and Data Capture (AIDC) is an industry term that describes the identification and/or direct collection of data into a computer system, programmable logic controller (PLC), or other microprocessor-controlled device without using a keyboard [1]. AIDC technologies provide a reliable means not only to identify but also to track items. It is possible to encode a wide range of information, from basic item or person identification to comprehensive details about the item or person e.g. item description, size, weight, colour, etc.

II. AIDC INFRASTRUCTURE

The Automatic Identification Data Capture (AIDC) infrastructure is defined as a set of networked devices and software components which include:

- Devices - include various identification technologies such as RFID reader, RFID printer, barcode scanner, sensors, and Programmable Logic Controller (PLC) etc.
- Services - are software components that enabling the data preparation, capturing, and processing.

Essential components of an AIDC infrastructure are identified and illustrated in the above diagram. It contains the following components:

- **Barcodes, Tags, and Sensors**: The smallest units that are attached to an enterprise entity or resource to be identified.
- **Device Controller or Edge Server**: A device controller is used to manage and control identification hardware (Readers, Scanners, Sensors and other Manageable Devices), aggregate, pre-process and cache the identification information.

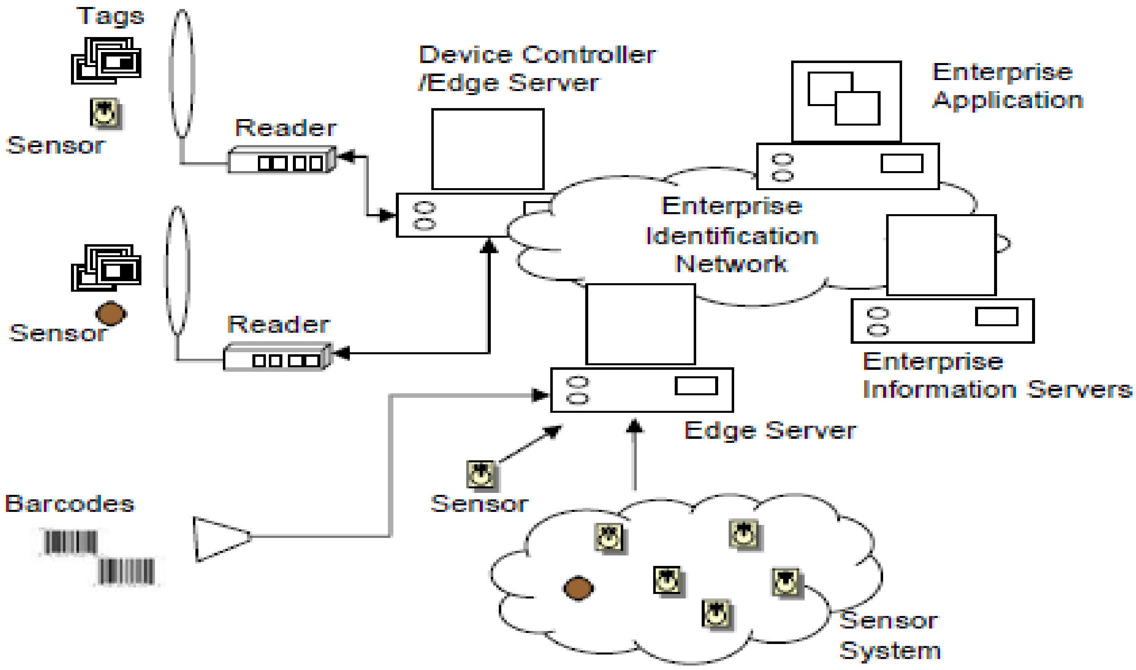

Figure 1: Components of AIDC infrastructure

- **Identification Network**: The identification network is the infrastructure that connects all the hardware resources and enterprise information systems together.
- **Enterprise Information Servers**: Enterprise information server provides enterprise activities related data which can be used along with the identification information for business operations. It provides real-time, aggregated identification data and events to client applications. The Enterprise Information System provides interfaces so that the application can define, register and look up events. It also provides interfaces that the end application can register and lookup production information, business information, and transaction information that is associated with a particular identification data.
- **Enterprise Application:** Enterprise applications are functional modules that full fill certain enterprise activities. For example, a Warehouse Management System uses the data captured by the Edge Server to monitoring the inventory level; an Asset Management System uses the data to look up a particular asset; etc.

III. BENEFITS OF AIDC

The key objectives of AIDC are [2]:

- Reduce data entry costs.
- Eliminate errors associated with identification and/or data collection.
- Accelerate the basic process.
- For moving assets, be able to collect tracking data and determine its exact location.

IV. AIDC TECHNOLOGIES

One or more than one of the following technologies are involved in an AIDC solution [2]:

1. Bar Code Technologies.
2. Radio Frequency Identification (RFID) and Data Communications Technologies.
3. Magnetic Ink Character Recognition (MICR).
4. Optical Character Recognition (OCR).
5. Optical Mark Recognition (OMR).
6. Electronic Article Surveillance (EAS).
7. Biometric Identification – Fingerprint, retinal scan or voice.
8. Contact Memory.
9. Machine Vision Technologies.
10. Real Time Locating Systems.

4.1. Bar Code Technology

Since its invention in early 1950s, bar code technology has accelerated the flow of products and information within a business and between businesses [2]. As a result of improvements in data accuracy that accompanies the adoption of bar code technology over conventional keyboard data entry; bar code systems have become critical elements in conducting business in today's national and global economies [3]. Bar code technology comprises of the following components:

- Symbologies that encode data that can be optically read by bar code readers.
- Printing technologies that produce machine-readable symbols.
- Scanners and decoders that capture visual images of the symbologies and convert them to computer-compatible digital data, and the verifiers that validate symbol quality.

The various bar code symbologies differ both in the way they represent data and in the type of data they can encode: some only encode numbers; others encode numbers, letters, and a few punctuation characters; still others offer encoding of the 128-character, and even 256-character, ASCII sets. The newest symbologies include options to encode multiple languages within the same symbol; allow user-defined encoding of special or additional data; and can even allow (through deliberate redundancies) reconstruction of data if the symbol is damaged.

Limitations of Bar code

- While there were over 200 bar code symbologies, only a handful of these are in current use and fewer still are widely used.
- However, given the low cost and immense investment in the current infrastructure, magnetic stripe is not expected to disappear any time soon.

4.2. Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is a relatively new AIDC technology that keeps track of anything, especially those assets that move. RFID is a portable memory device on a chip that acts like a Universal Product Code (UPC), is more than UPC because this microchip can carry much more dynamic information. This inexpensive microchip can be embedded in any object that stores basic information about the item [4].

RFID employs Radio Frequency Communications to exchange data between the memory chip and a host computer. An RFID system typically consists of a "Tag/Label/PCB" containing data storage, an Antenna to communicate with the Tag, and a Controller to manage the communication between the Antenna and the PC.

Greatest potential of RFID is in commercial and military supply chain applications where the process of tracking can be completely automated without a worker physically scanning an object, as is the case with UPC bar code scanning [5].

Limitations of RFID

- Data manipulation of RFID supply chain systems is quite difficult because of thousands of parts, and many location sensing points.
- Integration with existing supply-chain backend systems is still a problem. Some vendors have XML-based solutions in this area.

4.3. Magnetic Ink Character Recognition (MICR)

Magnetic ink character recognition (MICR), which was developed in the mid-1950s, is widely used in the banking industry for marking bank cheques. Routing and account information, including bank number and cheque number, are printed in stylized human-readable characters with ink that has magnetic properties [6]. The characters can be read by specialized magnetic readers even if they are overprinted by cancellation marks or smudges. This equipment, which must make contact with the characters in order to read them, requires precise registration and orientation.

Limitations of MICR

- MICR characters are very limited to only 14 characters.
- Any damage to the MICR characters or any printing out of the precise format specifications will cause a failure of the MICR print to be read properly.

- MICR scanners are also very precisely designed machines that are relatively expensive and need constant maintenance to maintain their reliability.

4.4. Optical Character Recognition (OCR)

The evolution of high-powered desktop computing has benefited OCR reading technology over the last few years, allowing for the development of more powerful recognition software that can read a variety of common printer fonts. High-end systems use sophisticated neural networks, which enable the system to improve its read accuracy over time by learning the nuances of a particular font and even varying styles of unconstrained handwriting [7]. Most OCR systems today are font-independent and are available in three different configurations: page readers, transaction readers (usually numerical only), and handheld readers.

Characters are scanned with a light source, providing an image that is interpreted by the recognition software. The software uses one of two approaches to character analysis: template matching (whereby the character is matched to a database of possibilities) and feature extraction (analyzing structural elements of the character) [2].

OCR shines in applications where human-readability is required, in electronic document processing and management, and in high-volume scanning of numerical transaction data. Neural net-based OCR systems are making headway in reading unconstrained handwriting, but such systems are as yet substantially inaccurate and prohibitively expensive.

However, OCR will continue to serve and grow in its established niches, particularly in electronic document processing and management applications, and in those industrial applications where the lack of human-readability of bar code symbology rules it out as a suitable technology.

Limitations of OCR

- For large commercial applications, font-independent OCR systems are considerably less accurate than those dedicated to an OCR font, and even a dedicated OCR system is less accurate than a barcode-based system. For this reason OCR technology is not likely to have a great impact on AIDC applications.
- Variety of character formation techniques, primarily printer-based technology, with costs determined by the type and quality of printer.
- Generally close proximity scanning required to capture images
- No encoded error control (error detection and correction) - reliant upon processing capability for recognizing characters

4.5. Optical Mark Recognition (OMR)

Most of us are quite familiar with this type of data input technology. As students, we have gone through standardized testing that uses optical mark recognition. This is one of the earliest types of automated data entry. OMR processes marked data by detecting and measuring reflected light flooding the form. When a mark has been made within a constrained area, it absorbs light [8]. Subsequently, electronic circuitry recognizes the mark as valid and sends a digital signal to the computer. The form data, represented by mark positions, are translated to ASCII text records for use in a variety of applications.

Another huge application of OMR is in lotteries, where participants can quickly and easily mark their selection of numbers on a machine-readable ticket. Although less sophisticated than other optical data collection technologies, OMR can serve certain high-volume data collection applications very cost-effectively because of labour and cost efficiencies. It has a lock on the educational market and is growing steadily in commercial and government applications.

Limitations of OMR

- Application-specific format are required
- Accuracy determined by the effectiveness of detecting marks and accommodating the variability in marks.

4.6. Electronic Article Surveillance (EAS)

This is technology used to identify items as they pass through a gated area [1]. Typically this identification is used to alert someone of the unauthorized removal of items from a store, library, or data centre. There are several types of EAS systems and more information is here on those different technologies. In each case, the EAS tag or label is affixed to an item. The tag is then deactivated when the item is purchased (or legally borrowed) at the checkout desk. When the item is moved through the gates (usually at a door to the premises), the gate is able to sense if the tag is active or deactivated and sound an alarm if necessary.

EAS systems are used wherever there is a chance of theft of small to large items. By placing an EAS tag on an item, it is not necessary to hide the item behind locked doors and so makes it easier for the consumer to review the product [9]. Today's hot topic in EAS is source tagging, where the tag is built into the product at the point of manufacture or packaging. This makes the labelling of goods unnecessary, saving time and money at the store.

4.7. Biometrics

Biometric identification encompasses a range of technologies that verify or recognize a person’s identity based on unique personal characteristics. It uses a physiological trait, digitally encoded and stored, to accomplish this identification. Biometric systems may simply identify the individual or allow a system to tap into a whole range of "rules" regarding that person. This data may be stored in a variety of formats including smart cards, or in the form of a two-dimensional symbology [1].

Most Biometric systems are used as a means of authentication when a primary means of identification, such as a card, is presented. Other more sophisticated systems are employed for primary identification, requiring no cards, passwords, or PINs. These "automated positive identification" Biometric systems prevent multiple enrolments by capturing, recording, and comparing an individual’s physical trait against an entire database as opposed to checking one record for a match. The cost and complexity of these types of Biometric systems have tended to limit their use to security applications, but as cost comes down, and processing power continues to increase, these systems will see more general use.

For Biometric identification, selection of a stable physical characteristic is key. Stable characteristics include the user's hand silhouette, a facial feature, iris pattern, a blood vessel pattern on the retina or hand, and of course, a fingerprint. Individual behaviours may also be used for biometric identification [10]. Behavioural identification may be achieved by analyzing signature dynamics e.g. how one types on a keyboard, or how one speaks (voice patterns). For example, signature dynamics differentiate the parts of the signature that are habitual from those that vary every time you sign your name. Because behavioural characteristics vary over time, behavioural-based equipment may update users' enrolled Biometric reference templates each time they access the system. With each use, the machine becomes increasingly proficient at identifying an individual.

Performance of Biometric systems is measured by their identifying power, which is calculated using false-rejection and false-acceptance rates. Biometric identification systems allow users to set the desired balance of false-rejection and false-acceptance. If this tolerance is tightened to make it harder for imposters to beat the system, it is also harder for authorized people to access it. Biometric experts state that thorough user training is the best way to reduce false rejections. Knowing and optimizing a system's identifying power, and making sure it is acceptable for your application and in your industry, is critical for system success. For example, adoption of automated signature verification for credit card and check applications has been slow because the financial community demands very low false rejection rates.

Limitations of Biometrics

- More biometric technologies that have disadvantages linked to them include voice, signature, and hand geometry verification.
- With voice verification there needs to be as little background noise as possible or the spoken phrase will not be registered accurately.
- With signature verification the problem happens when people's signatures change over time and are not always consistent.
- And lastly, hand geometry verification is a high cost service and needs device of a large size to carry out the task
- Different biometric technologies need the use of different devices that have a range of costs.

4.8. Contact Memory

A contact memory device looks like a small button-style camera battery, but it's really a stainless steel container with a memory chip sealed inside. The top of the button is bonded to one point in the memory circuit; the bottom and sides of the package provide a signal ground. Data is written to and from the button using a probe-like device that is touched to the two electrical points on the unit, thereby establishing a communication path [1]. A button can act as a "license plate" identifier or as a portable database in which data can be read and modified.

The buttons generally come with a unique pre-programmed identification number and are available in a variety of memory configurations. They can hold up to four million bytes of reprogrammable data, including text, pictures, and even voice messages. This data may be transferred to a computer via a button reader at speeds up to 16.6 Kbps. Buttons may be set with a password to protect the data from being read or rewritten.

Some buttons are powered by small internal batteries that guarantee data retention for 10 years from date of manufacture. Other battery-free designs retain data up to 100 years, and each time the button is read, a small amount of additional power is transmitted to it, further extending its memory. Buttons are sealed to withstand moisture, radiation, and temperature extremes, and operate under a wide range of temperatures.

Contact memory technology will continue to be employed in cutting edge applications ranging from electronic purses, research, and electronic product identification, to collecting oil production data in the field. Users (and manufacturers) will combine buttons with other technologies in creative ways to enhance their AIDC applications. For example, one type of button incorporates a digital thermometer that can measure temperatures from -55 ºC to +100 ºC, typically in one second. Users can place these sensors to obtain a temperature profile of a piece of equipment, a room, or a building [10]. Touch/button memory is a relatively simple AIDC method whose use is limited only by a user's inventiveness.

Limitations of Contact Memory

- Low to relatively high data storage capability.
- Data transfer rate determined by systems and serial interface.
- Relatively small application base

4.9. Machine Vision

Video camera-based machine vision systems have been used for industrial inspection and quality control for a number of years. However, they have only recently been integrated into AIDC applications because 1D linear barcodes were scanned far more cost-effectively with laser scanners. The recent development and use of 2D matrix barcodes has rapidly driven technology refinements and cost-efficiencies in vision-based scanning used for AIDC applications [2].

Vision-based scanners use a CCD-based video image, very similar to a video camera, to capture an image and convert it into a digital format. Fluorescent lighting, high-speed strobe flash, or an array of LED’s, most usually provides the illumination source. Specialized electronic circuitry and/or software processes the digitized image to obtain the encoded data.

Decoding algorithms have been developed for both 1D and 2D symbologies (as well as for Optical Character Recognition applications). Because a vision-based system captures a symbol’s complete image, more information is gathered than can be obtained from a single or raster-scanned laser beam. Processing this wealth of information allows for reading at lower contrast ratios and a greater ability to work around impairments.

Limitations of Machine Vision

- Application specific processing generally required.
- Can be cost effective in applications where continuous automated inspection is required and the technology is applied as part of a statistical process control system.
- Illumination can be an important consideration.

4.10. Real Time Locating Systems (RTLS)

For centuries organizations have faced the challenge of locating and tracking inventory and assets by brute force. The activity of receiving, storing and issuing inventory items and tracking the use and location of capital assets has remained essentially unchanged. Whether by quill and scroll; pencil and clip board; or bar code scanner and database, the process is fundamentally the same: receive items, put them away, refer to some kind of list and then find them [2]. Along the way items get misplaced, moved, lost, or forgotten. Some organizations have described their warehouse inventory process as moving products from one black hole to another.

Imagine the challenge of trying to find the exact location of one of thousands of containers in a large area where all of the containers essentially look alike. These containers may be as small as a pallet or as large as a trailer truck. While traditional technologies can help record when a container was received and where it was delivered, no system has been able to provide accurate real time location information to the managers of complex operations. No system, that is, until the introduction of Real Time Locating Systems (RTLS).

Real Time Locating Systems are fully automated systems that continually monitor the locations of assets and personnel. An RTLS solution typically utilizes battery-operated radio tags and a cellular locating system to detect the presence and location of the tags. The locating system is usually deployed as a matrix of locating devices that are installed at a spacing of anywhere from 50 to 1000 feet. These locating devices determine the locations of the radio tags.

The systems continually update the database with current tag locations as frequently as a few seconds or as infrequently as every few hours for items that seldom move. The frequency of tag location updates may have implications for the number of tags that can be deployed and the battery life of the tag. In typical applications systems can track thousands of tags simultaneously and the average tag battery life can be five or more years.

V. TECHNOLOGY AND BUSINESS TRENDS

Until now, AIDC industry has been focusing on scanning (bar code and other technologies described on our pages). However, we see following trends [2]:

- **More standardization in OS**: Portable data terminals being based on more powerful and more open operating system standards. Unique low-level OS modifications and device drivers are being replaced by industry-standard device drivers supported by Windows CE, PalmOS, Symbian EPOC, etc. AIDC vendors are becoming product and device systems integrators.
- **Both Industry-Specific and General Purpose Portable Devices** - not only industry specific devices are being designed but many general-purpose devices like Palm and Handspring are being equipped with scanners. Added value comes through functional-enhancing software from AIDC vendors like Symbol e.g. SPT 1500 adds scanning to Palm devices
- **RFID taking over from manual scanning** high-value asset location applications
- **More Wireless LAN** connected devices
- **More IEEE 802.11**-based (a wireless LAN standard) devices - AIDC vendors are giving up unique wireless LAN standards in favour of industry-standards LANs
- **More integration between AIDC applications and supply-chain applications**

VI. COMPARING VARIOUS COMPONENT TECHNOLOGIES

Because of the diversity of solutions offered by AIDC technologies, there is no single technology that can be considered the "best" component technology [10]. The "best" component technology for product identification in one application may not be the "best" component technology in another situation. Matching these capabilities to your data collection needs is really the only way to choose the "best" component technology. Your challenge is to combine several technologies together to meet the requirements of a specific business problem.

VII. CONCLUSION

A variety of identification technologies have been used in the enterprise systems to improve the enterprise operation efficiency and reduce the overall operation cost. Barcodes, RFID, and sensors are the most commonly used and important technologies that have been addressed. Because of its low cost, today, the barcode is the major identification technology used by most enterprises. The emerging RFID technology brings significant new opportunities as well as challenges to the AIDC infrastructure. The combination of RFID and sensor technology brings additional value to the enterprise operations.

The challenges to AIDC are: The performance of data capture and processing; the manageability and extensibility of heterogeneous devices; scalability and performance of the AIDC infrastructure; Discoverability and availability of resources; the integration of various identification resources with the diverse EIS. The extensibility, scalability, resources usability and discoverability, RFID system performance, device manageability, and system integration ability of AIDC infrastructure are important topics of current AIDC research.

Regardless of the AIDC technology you employ, a wise choice regarding consumables is the front-end decision that will keep your application running economically and smoothly into the new century. Developments in the consumables arena focus on durability and environmental issues. In an effort to support the global recycling movement, AIDC manufacturers continue to explore ways to produce less waste and efficiently recycle the waste materials that are produced. Additionally, users continue to demand more from their systems and durable labels, tickets, cards, and tags are key pieces of those systems.

VIII. ACKNOWLEDGEMENT

I thank THE LORD Almighty for guiding and showering HIS blessings throughout my life and this paper in particular. I genuinely thank our Mother Mary for her powerful negotiation. I would like to thank my husband for his love and support. I thank my parents for their patience and care. I am so grateful and appreciative of all those who have helped and supported me in this venture.

REFERENCES

[1]. http://en.wikipedia.org/wiki/Automatic_identification_and_data_capture
[2]. http://mobileinfo.com/AIDC/index.htm
[3]. Bar codes, http://www.lintech.org/comp-per/06BARCD.pdf
[4]. GS1 US, The Universal Product Code, http://www.uc-council.org/upc_background.html

[5]. K Finkenzeller, G Munich, *Radio-Frequency Identification*: *Fundamentals and Application, RFID Handbook*, Wisley & Sons, 1999

[6]. http://www.slideshare.net/Etilux/aidc-solutions-references

[7]. A.D. Smith, F. Offodile, "*Information Management of Automatic Data Capture: An Overview of Technical Developments*", Information Management & Computer Security, Vol. 10, No. 2-3, 2002, pp. 109-118.

[8]. A. Gunasekaran and E.W.T. Ngai, "*Build-to Order Supply Chain Management: A Literature Review and Framework for Development*", Journal of Operations Management, Vol. 23, No. 5, 2005, pp. 423-451.

[9]. B. Subirana, C. Eckes, G. Herman, S. Sarma and M. Barrett "*Measuring the Impact of Information Technology on Value and Productivity using a Process-Based Approach: The case for RFID Technologies*", MIT Sloan, Working Paper, December 2003, Retrieved May 15, 2004, from www.papers.ssrn.com/sol3/papers.cfm?abstract_i =478582

[10]. C. Bornhövd, T. Lin, S. Haller and J. Schaper, "*Integrating Automatic Data Acquisition with Business Processes Experiences with SAP's Auto ID Infrastructure*". Proceedings of the 30th VLDB Conference, Toronto, Canada, 2004, Retrieved March 05, 2007, from: http://www.vldb.org/conf/2004/IND6P1.PDF

AUTHOR 'S BIOGRAPHY

Anto Ramya. S. I was born in Cochin, Kerala (KE), India, in 1985. She received the Bachelor of Commerce (B.Com.) degree from the Periyar University (PU), Salem, TN, India, in 2005 and the Master of Computer Applications (M.C.A.) degree from Anna University, Chennai, TN, India, in 2008 and Master of Philosophy(M.Phil.) of Computer Science Degree from the PU, in 2012. Her research interests include neural networks, mobile computing and MANET.