



TRENDS IN ACCESS CONTROL

1. INTRODUCTION

I have been involved in the Access Control industry for the past decade. My involvement was at first as a user, then a system integrator, and in the recent years, a manufacturer. In the early days, it was a hobby to me to follow the trend of development of the access control industry. In the recent years, this however has become a very important part of my responsibility in my place of work. As a manufacturer of Card Access Equipment, it is important for me not only to know the trend, but also to predict the trend and hopefully to produce products in step with the trend.

This is not a technical paper, in that I do not discuss any particular technology at any great depth. It is not commercial, in that I am not trying to sell ELID or any other brand. Rather it is a forecast of how I think this industry will develop and impact us, particularly in South East Asia in the coming years. The background materials are gathered from a wide range of literature - brochures, technical articles, data sheets, as well as from exhibitions, talks, and seminars.

2. AUTOMATIC IDENTIFICATION - The Starting Point

The starting point of all Access Control Systems is automatic identification - the process whereby the identity of a person is presented and read by a machine in a reliable and secure way. Put it in another way, the choice of a reader and the accompanying token or card to be carried by each person. The conventional bar-coded cards and magnetically coded cards have served us well and will no doubt continue to be used for many more years to come. But there is a strong undercurrent of growth in other automatic identification technologies, especially proximity technology.

3. BIG PLAYERS

Proximity cards are not new. Schlage, an American company, has been supplying such cards and readers for a long long time. Other companies such as Cotag of UK, Deister of Germany, Matra Communication of France have also been producing proximity cards for some years. But recently, something exciting is happening, in that for the first time, big players are coming into the picture. For example, in March 1991, Texas Instruments, a company with 60,000 employees worldwide, announced its entry into this market with the introduction of TIRIS (Texas Instrument Registration and Identification System). Texas Instruments claimed that it has 250 employees involved in engineering, marketing and manufacturing TIRIS. Motorola, another top ranking multi-national company has recently bought over Indala, a small specialist company located in California, which has been producing proximity cards for a number of years. GM-Hughes Electronics, another giant American company has also entered the same market sector. These companies are from USA alone. Many other major players from Europe and Japan are also entering this market.

4. SMART PROXIMITY

Traditionally, proximity tokens are 'read-only' devices, in that the code inside is programmed during manufacture and the code can only be read by the reader and cannot be altered by the reader. Furthermore, the number of bits of information is quite limited. This is rapidly changing. A number of manufacturers today are offering tokens of much higher capacity with the ability of changing the code (writing) in a fraction of a second.

From a totally different market sector - the smart card market, development is progressing which overlaps into the traditional proximity card market. The conventional smart card consists of an IC chip embedded in a plastic card, the card has to be read by physical contacts. Recently, cards are available from a number of companies, e.g. GEC, which are contactless, working on the same principle as proximity cards.

What is the difference between memory type smart card and proximity cards with read-write capability? Very little, except perhaps memory size. Yet they have evolved from 2 different industries. What has happened is that the proximity card makers have adopted the use of EEPROM read/write technology from Smart Card manufacturers and Smart Card manufacturers have adopted the radio frequency remote activation technology from the proximity manufacturers, and they end up with virtually the same product.

5. GROWING APPLICATIONS

When Apple first introduced its PC, it was supposed to be for computer hobbyists. The inventors never dreamt that one day, the PC was going to change the work pattern of virtually every person on earth. I believe that another significant revolution is at hand, which will also affect each person in this world, spurred by the new generation of smart proximity cards.

Most of us are familiar with the use of identification tokens for access control. They are 'keys' that allow us to enter car parks, offices, lifts etc. They offer a number of advantages that conventional keys cannot provide. For example, the ability to put "time zones" whereby the 'keys' can only be used on selected days between selected times, the ability to log the identity of who have entered into a particular door, or tracking the whereabouts of a person, and printing out his movements; or cancelling a person's right to enter a certain door in seconds.

Most of us are also familiar with the use of identification tokens for credit control - credit cards, bank cards, club membership cards etc, that allow us to identify ourselves and gain access to banking facilities, credit facilities, or club facilities.

We are also familiar with the use of prepaid cards; phone cards, transportation (transit) cards, parking cards etc, where the amount of money stored in the card is successively deducted as we use the facilities provided.

Keys, credit cards, and prepaid cards are carried by virtually every person. Is it too far-fetched to imagine that one day, all these will be replaced by a single smart proximity token? A single token that will act as key to doors, that authorizes credit billing for purchases and phone calls? And when this has happened, is it not logical, as a next step, to make that same token to contain also particulars of our identity card, driving licence, and passport?

The application of automatic identification is not limited to people only. Animals, factory products, factory processes, vehicles etc also need identification. Attaching identification token to a cow or a sheep to track its growth has been in use for a long time. Products under manufacture (e.g. cars in an assembly line) can be tagged by identification tokens so that their production progress can be monitored. More and more commercial vehicles in western countries are tagged by identification tokens so that they can be automatically identified during refuelling. The scope of application of automatic identification continues to multiply, limited only by our imagination.

6. OBSTACLES

What are the problems that we still need to face in the days ahead before the explosive growth of identification tokens can take place ?

Firstly, there is the problem of standardization. To date, there is no standardization of hardware and there is no standardization of data formats between the security industry and other industries (e.g. banking industry). Even within the security industry, there is no standardization of data formats. The so-called "Wiegand compatible" signalling has become the effective standard for hardware, simply because it provides the easiest and fastest means of adapting proximity readers to existing controllers. However, Wiegand format is no longer adequate, particularly if the token is also to cater for write operation. In order that a single card may be used for security industry, banking industry, telephone and transportation industry, there must be cooperative effort to evolve a standard which should be undertaken at the global level.

Secondly, there is the matter of cost. Smart Proximity cards and readers, despite their many advantages, are still too expensive for most countries in South East Asia. As a result, magnetic cards and readers, which are an order of magnitude cheaper, still have the lion share of the market, and will continue to do so unless the price of Smart Proximity cards and proximity readers drops drastically.

Thirdly, there is the difficulty of system integration. Even the use of a single-purpose card (e.g. access control) in a large organization requires significant hardware and software expertise. When this is extended to multiple functions, involving different industries, each requiring a high level of security and exclusivity, the system integration effort is multiplied many times.

7. CONCLUSIONS

Pragmatism requires that we look at the now - What must I do if I were to plan for an access control system now? I believe that it is imperative for the access control consultants and system designers NOT to view access control as the end-all and be-all, but rather as only the first step into something that can grow year by year. For example, in a factory environment, what may start as a door security system this year, can expand into time attendance control next year, and production tracking the year after, and factory meal subsidy scheme the next etc, all hinging on the "one-card" concept.

It is difficult to implement all the facilities in one go simply because of the learning process required. Over ambitious may end in excessive delays in implementation as success is as much dependent on cooperation of the employees as it is on system performance. It is wiser to implement in stages so that users are confidently brought from one level of sophistication to the next.

On the other hand, to implement a system without planning for long term expansion is not wise. For example, one may have chosen an ID technology that is not secure enough to cater for new applications that come about a few years down the road; or one may have chosen a supplier that does not provide sufficiently wide coverage of equipment to cater for new needs. In both the above cases, one may be forced to abandon the old system and purchase a brand new system so as to be able to implement new applications, an expensive and time consuming process.

I also believe that for many more years to come, access control will continue to be the largest user of automatic identification technology. Therefore, the access control industry must prepare itself to grow as automatic identification applications grow. Otherwise, there will be a danger that access control industry will lose the lead and be overwhelmed by newcomers from other industries who too use automatic identification technology.