Application of Tracking Technology to Access-control System

OVERVIEW: An access-control system that applies tracking technology to control the movement of people and goods inside buildings has been developed. This system — whose key components are a newly developed, ultralow-power-consumption infrared transmitter/receiver and a weak-radio-wave RFID (radio-frequency identification) tag that can handle infrared and RFID signals at the same time — can precisely detect the passage direction of each tag carried by individual people or fixed to items moving in a line. Applying this system to access control has made "hands-free" room access possible. As regards conventional systems utilizing smart cards and biometrics, it is a concern that their security level and user convenience are conflicting issues. In contrast, placing no burden on the convenience of the user at all, the developed hands-free access-control system can provide efficient access control at higher precision. With the aim of promoting new physical-security technologies that have been unavailable till now, the current paper first overviews the main features of the system and then describes two examples of its implementation.

INTRODUCTION

IN the past few years, car-navigation systems have created a huge market in what seems like in no time at all. And regarding systems for outdoor tracking and location, in addition to such GPS (global positioning system)-based car navigation, systems utilizing mobile phones and PHS (personal handyphone system) are being practically applied.

On the other hand, regarding location systems for indoors, although systems utilizing PHS and active RFID (radio-frequency identification) have demonstrated positive results, they have not reached the stage of widespread use because of problems with handset size and location precision. If high-precision "indoor-use tracking" utilizing compact tags were realized, various applications such as location systems like car navigation would be possible. In particular, if the conventionally difficult "people tracking" were realized, the range of possible applications in various kinds of businesses, such as security, distribution, and safety, would widen.

In response to the above circumstances, Hitachi has developed a "dynamic-state-monitoring system," whose key component is a newly developed RFID tag that utilizes infrared radiation and long-distance radio-wave communication. Taking a global lead, we are offering this system as a new kind of tracking system (see Fig. 1).

APPLICATIONS OF ACCESS-CONTROL SYSTEM

Conventional access-control systems use a card reader to scan magnetic cards, smart cards, etc. in order to authenticate the card holder. On authorization of the ID (identification), the electric lock on the door is unlocked and the door can be opened. This procedure is essentially no different from the conventional use of a key. Against the backdrop of concerns regarding social unrest and protection of business information, access-control systems must satisfy an increasing diversification of needs.

To realize a high reliability, smarter, and more efficient access-control system (which is not just a substitute for a key-based system), it is necessary that users of facilities are not conscious of using the system; in other words, authentication must be performed while a person is naturally entering a room. The main feature of the developed system is that it meets this requirement by providing "hands-free" access control (see Table 1).

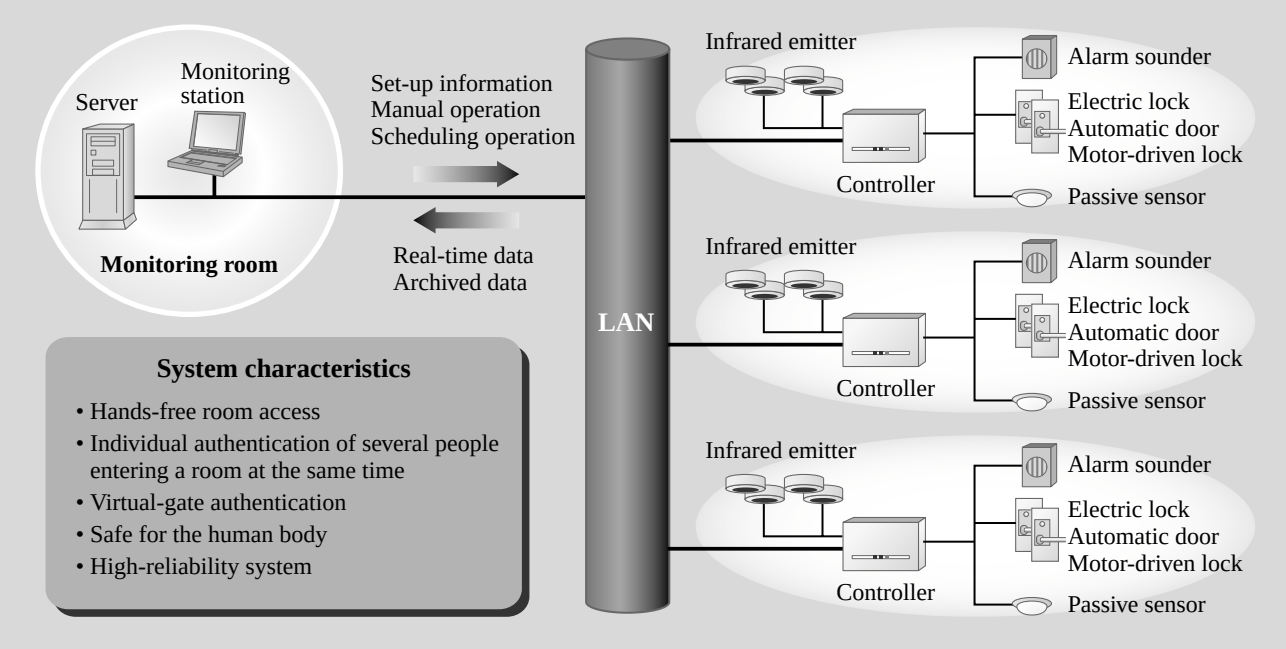

Fig. 1—Configuration of Access-control System Applying Tracking Technology.
This autonomous distributed system is configured so that each gate is controlled by a dedicated controller and the whole system is under the unified control of a PC server running UNIX. The system not only provides gates that are physical barriers but also performs access control by means of virtual gates.*

TABLE 1. Comparison with Other Systems
This table compares our system with other systems in terms of major features. Note that location management and simultaneous reading are features unique to our system.

Feature	Our system	IC card	Biometrics
Location management	Yes	No	No
Hands free	Yes	No	Depends on system
Simultaneous reading	Yes	No	No
Reading accuracy	High	Low	Somewhat low
Responsiveness	Fast	Fast	Slow

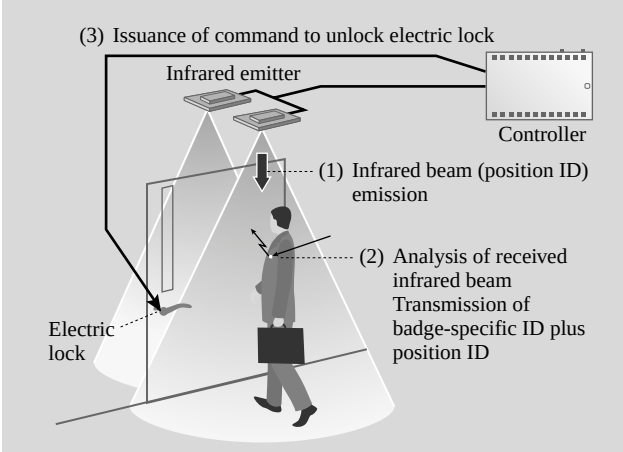

Fig. 2—Principle of System.
The basic operation principle of the verification of the badge-specific ID and the unlocking of the electric lock is shown.

SYSTEM CHARACTERISTICS

Hands-free Room Access

To accomplish hands-free room access, a transmission and reception system utilizing infrared radiation and long-distance-communication RFID was developed. The basic principle of the system is shown schematically in Fig. 2. When a person wearing the developed RFID badge stands in front of the room he/she wants to access, the system assesses whether or not that person has access authorization. In the case that authorization is given, the door is unlocked and the authorized person gains access. This procedure consists of the following three steps [indicated by the numbers (1)–(3) in the figure]:

(1) An infrared emitter at each checkpoint (spot) continuously emits an infrared beam forming a particular signal as a unique "position ID" for each spot.

(2) When a person wearing a badge passes through a

* Unix is a registered trademark of The Open Group in the United States and other countries.

spot, the badge picks up the infrared beam and extracts the position ID from it. The ID specific to that badge and the position ID are then combined, and the combined ID is transmitted as an RFID signal.
(3) The controller receives the combined ID and separates the specific ID and the position ID. By doing so it can ascertain which particular badge has entered any particular spot. It then checks the specific ID against the security level for the door in the spot in question. If it confirms that the ID has access authorization, it issues a command to release the electric door lock.

In this way, since authorized persons follow the above procedure without being aware of it, they can access authorized areas freely in a "hands-free" manner, and security checks can be carried out on them without inconveniencing them.

Individual Authentication of Several People Entering Room at Same Time

By providing hands-free room access according to the above-described principle, we have overcome what has been a key issue up till now, namely, individual authentication of several people entering a room at the same time. Fig. 3 shows an image of such an access situation.

As regards a conventional system, access is controlled by means of smart cards, etc. However, in this case, it is possible that when the person in the front of a line of people is authenticated and the door is opened, the persons immediately behind them can enter without being authenticated. On the contrary, in the case of the newly developed system, each person in the line can be individually authenticated.

Virtual-gate Authentication

The new access-control system also makes it possible to carry out authentication without the need for physical gates. That is, an authentication system consisting of so-called "virtual-gates" can be set up as shown in the image in Fig. 4. In this system, areas are separated into zones by virtual gates that perform "soft" security checks (i.e. non-doorway checks) in order to provide a high level of access control.

Even in door-less, spatial places like corridors, virtual gates can be set up in order to automatically authenticate anyone passing through. If an unauthorized person or someone not wearing a badge is detected, a warning announcement is given and the image of that person is recorded by a surveillance camera.

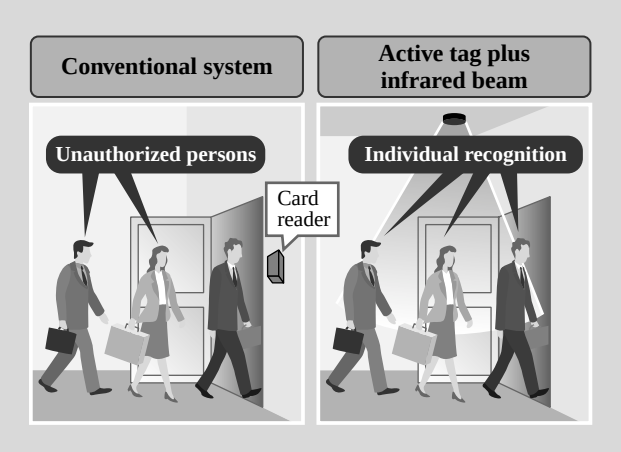

Fig. 3—Individual Authentication of Several People Entering Room at Same Time.
As regards a conventional system, access is controlled by means of smart cards, etc. In this case, it is possible that when the person in the front of a line of people is authenticated and the door is opened, the persons immediately behind them can enter without being authenticated. By contrast, in the case of the newly developed system, each person in the line can be individually authenticated.

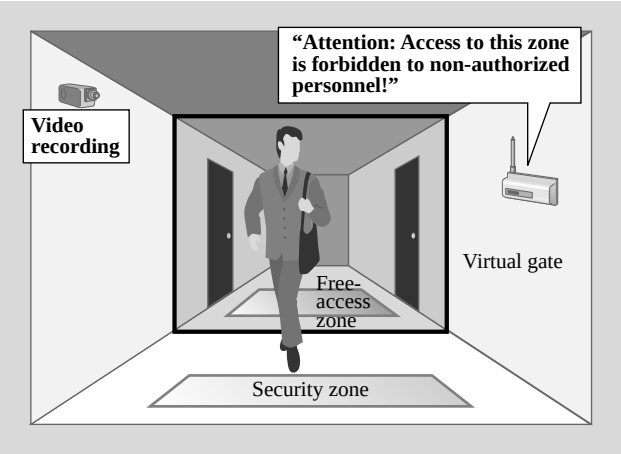

Fig. 4—Virtual-gate Authentication.
Even in door-less, spatial places like corridors, virtual gates can be set up in order to automatically authenticate anyone passing through. If an unauthorized person or someone not wearing a badge is detected, a warning announcement is given and the image of that person is recorded by a surveillance camera.

Badge Security

The badge used in the developed access-control system provides a high level of security by utilizing infrared radiation and an RFID device that produces a weak radio-wave signal. Though this weak radio-wave output power is 1/10000 of that of a standard mobile-phone signal, or 1/100 of a PHS signal output, it can

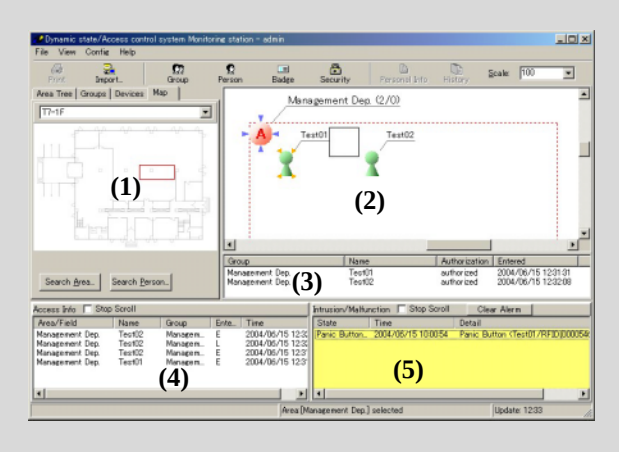

Fig. 5—Example Screen Image of PC Monitoring Station. The screen visualizes a particular facility. The numbered areas in the example image contain access information corresponding to the following: (1) the whole facility; (2) a close-up of the area enclosed by a red line in (1); (3) the people in that room; (4) records of room accesses; and (5) records of warning announcements.

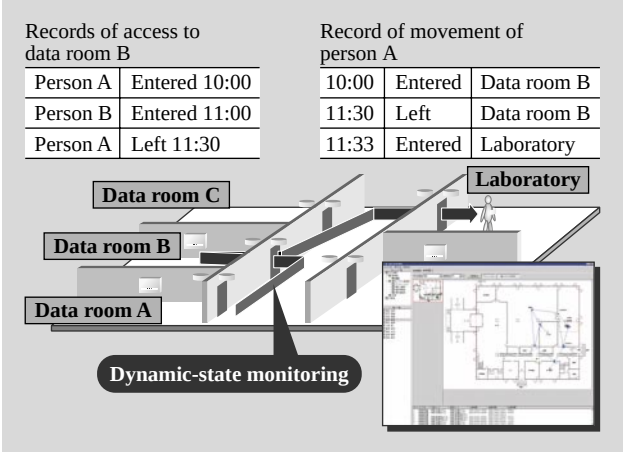

Fig. 6—Records of Peoples' Room Entry and Movements. Records for each room of each person's entry of and records for each person's movement (i.e. access or exit from each room) are accumulated. In this way, a visual image of each person's movements can be created.

still ensure a high level of security. By utilizing such a badge, the new system can be applied in hitherto difficult areas, like healthcare facilities, where use of such devices is restricted.

High-reliability System Configuration

Providing a system that ensures high reliability brings the two additional advantages listed below:
(1) Even if the server or network is down, autonomous decentralized control ensures that access control is continued without hindrance.
(2) With a platform consisting of an SH microcomputer without an HDD (hard disc drive) or cooling fan running a Linux*[1] operating system, the controller — the core of the access control — can provide long-term, stable operation.

Wide Range of Standard Interfaces

The developed controller is not just a basic device for controlling the infrared emitter and electric door locks; it can also be hooked up to standard multipurpose devices in order to control warning buzzers, voice guidance, and LCD (liquid crystal display) touch panels. By providing a standard application that functions as a monitoring station with a user-friendly GUI (graphical user interface), and that can be simply installed on a network-connected PC, dynamic-state monitoring and access control can be practically implemented. Fig. 5 shows an example GUI image for such monitoring and access-control operations.

The screen visualizes a particular facility. The numbered areas in the example image contain access information corresponding to the following:
(1) the whole facility;
(2) a close-up of the area enclosed by a red line in (1);
(3) the people in that room;
(4) records of room accesses and warning announcements.

Easy Multilingualization by Means of Multilingual Library

The system supports Unicode*[2], so access to a library of languages other than Japanese is simple. In the future, it is planned to support English and Chinese as standard from April 2005.

SYSTEM EXAMPLE APPLICATIONS

Installation of Security Centered on Dynamic-state Monitoring

The developed access-control system has been installed at sensitive facilities like research centers to provide a high level of security regarding internal staff and visitors. The main features of the system are listed below:
(1) Each area in the facility is defined hierarchically so that it is given a detailed security level.
(2) Organizations and outside people are defined in

*1 Linux is a trademark of Linus Torvalds in the U.S. and other countries.
*2 Unicode is a trademark of Unicode, Inc.

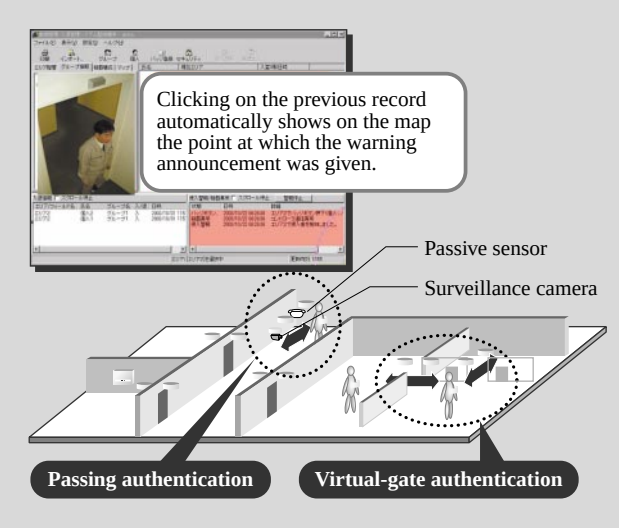

Fig. 7—Virtual Gate and Virtual Area.
A person's passage through corridors and movement within rooms are automatically detected, authenticated — and warning announcements can be given in real-time if necessary — and recorded as archive data.

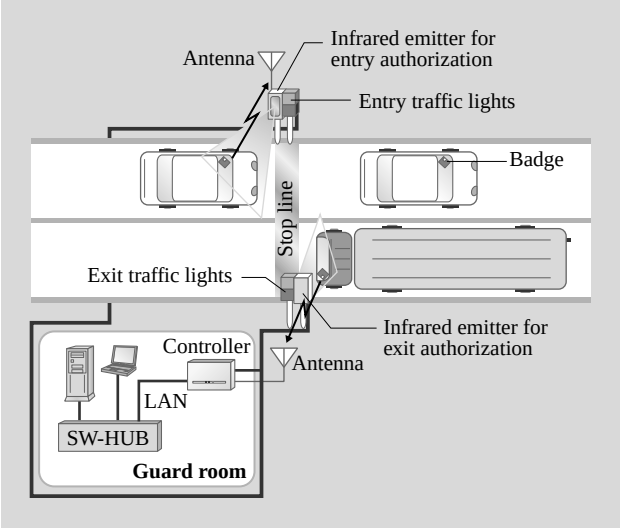

Fig. 8—Schematic of Vehicle-access-control System.
A vehicle equipped with an RFID badge is automatically authenticated at the barrier; if its authorization is confirmed, the barrier is raised or a green light is given.

groups according to vertical or lateral organizational hierarchy, and an "access level" for each location is given to each defined group.
(3) Record data on room access for each location and movement data for each individual or group are accumulated (see Fig. 6).
(4) Virtual gates are set up in building passageways, and if an unauthorized person is detected, a warning announcement is given and an image of the intruder is shown in real-time. In addition, virtual gates set up in the offices accumulate records of the movements of authorized people. If an unauthorized person passes a virtual gate, a notification message is sent to the person in charge and an image of the person is recorded simultaneously (see Fig. 7).

Proposed Vehicle-access-control System

In this proposed application, the developed access-control system is set up to connect barriers and traffic signals for controlling the movement of vehicles in places like industrial and public facilities or distribution and delivery warehouses. An RFID badge installed in each vehicle enables the authorization or non-authorization of each vehicle to be confirmed at the entry and exit gates of these facilities as well as at "area" gates set up along internal roadways. The gate barriers are then opened or closed and traffic signals are controlled according to this authentication. This is an example of the access control system developed for people being applied to vehicles. Equipping vehicles with previously registered badges and checking their authorization automatically means that the drivers do not have to get out of their vehicles. This helps the entry and exit of vehicles to be controlled smoothly around the clock. Compared to the current ETC (electronic toll collection) system, which is referred to as "non-stop," the proposed vehicle-access control system can be referred to as "one-stop." As this name implies, the proposed system is not as convenient as the ETC system. On the other hand, the tag cost and the system-installation costs are low, so it can be installed at any general business premises at low cost. A schematic image of the proposed vehicle-access-control system is shown in Fig. 8.

CONCLUSIONS

A newly developed access-control system — combining infrared radiation and an RFID tag — was focused on in this paper. Although only two typical applications of this system were briefly introduced, a wide variety of other applications in the areas of security control, product management, and personnel time management are also being provided. Moreover, by combining the developed system with a location system that uses only individual compact RFID tags, it will be possible to broaden the range of applications.

In the future, we intend to provide high-reliability systems — with higher accuracy — for indoor tracking of people and goods. As regards overseas markets, we plan to launch such systems from 2005 onwards.