



Rapid Deployment Access Control Systems

TRANSCORE.

Rapid Deployment Access Control Systems

Access Control Points at forward camps and military facilities require robust security. This paper describes a rapidly deployable trailer-mounted system, describes the methods of authentication, describes procedures for automating procedures and increasing guard security, and summarizes the technology required for such a system.

Forward camps and military facilities, such as those currently located in Kuwait, Saudi Arabia, Iraq, and elsewhere, require robust security at access control points. Those systems and technologies that are trailer-mounted for rapid deployment can be described as Rapid Deployment Access Control (RapDAC) systems.

A RapDAC system is designed for rapid deployment of secure access points with guard security at remote locations. These trailer-mounted systems allow security forces to set up remote access control points (ACP) and to issue windshield sticker tags to authorized vehicles. The minimum installation of a mobile trailer-mounted system includes a base trailer, access to a power supply (generator or cable power), a retractable mast to support an interrogator (often called reader) and signal lights, a gate or pop-up barrier, and a computing device called a lane controller.

The core function of a basic RapDAC system is to determine whether a vehicle is authorized to enter. The ACP uses radio frequency identification (RFID) technology to authenticate the vehicle's windshield sticker tag. The RFID reader transmits a radio signal. The vehicle's RFID sticker tag reflects a modulated signal, which the reader converts into a digital number that the software compares to a list of authorized IDs. If the software finds a tag ID match on the list of authorized IDs, the vehicle is authorized to enter. A RapDAC system can easily support additional methods of authentication. For higher levels of security, guards operating the RapDAC can be stationed remotely at a central station that has two-way communications with the ACP as well as video surveillance of it.

A RapDAC system is based on one or more authentication technologies to confirm the identity of vehicles and persons at secure access points. The authentication technologies include RFID for vehicle authentication, RFID or common access cards (CAC) for ID card authentication, and visual inspection or biometric measurement for entering person authentication. This paper discusses technology requirements according to the following criteria:

- Methods of Authentication
- System Automation and Guard Security
- Access Control Devices and Software

Methods of Authentication

The highest level of security at an access point requires two methods of authentication. The basic authentication method verifies entering vehicles, and the second authentication method verifies the persons inside the vehicle. Technologies for authenticating entering persons include ID card authentication and biometric readings or visual inspections to confirm that the person matches the ID card. Additional authentication protocols can confirm that a driver is authorized to drive the vehicle.

One method of authentication at an access point is the RFID sticker on the vehicle. For additional security, sticker tags can be designed so as to be disabled upon removal. To enter a secure location, a vehicle must have a tag with an authorized ID. Readers, which are located at the secure access point, may also be

deployed forward also to verify that an approaching vehicle carries an authorized RFID sticker. This method of authentication is basic to a RapDAC installation.

The second method of authentication confirms the identity of the entering person. This method uses any of the following protocols to provide additional security: confirm that the entering person is authorized to enter and carries a verified ID card, confirm the entering person's physical characteristics using either visual or biometric confirmation, and/or confirm that the vehicle driver and passengers are authorized to travel in the entering vehicle.

A RapDAC system should provide flexibility in setting the protocols for confirming the identity of entering persons and their authorization to use a vehicle. CAC cards can use standard protocols, and RFID-based access cards can be read with the same technology that reads secure sticker tags. Remotely located guards can use video cameras to inspect vehicle occupants or hand-held biometric devices to match the card holder's fingerprints to fingerprints stored in the database. System flexibility should allow both that multiple vehicles can be associated with an authorized driver and that multiple drivers can be associated with an authorized vehicle. A combination of multiple technologies for confirming the card presenter's characteristics and authorizations provide robust security in a RapDAC installation.

A RapDAC installation includes the following devices:

- CAC readers or RFID-based card readers
- Biometric identification devices that can be carried in the vehicle or mounted at the access points
- Remotely controlled video camera to identify the driver and remotely controlled vehicle inspection or remote tracking cameras (digital or standard)
- Lane devices so that a lane controller can detect a vehicle's presence and its direction of travel. These devices include loops, light curtains, and treadles. Loops are underground cables that detect a vehicle's presence. A light curtain has an infrared beam that reports the presence of object. Treadles are pressure-sensitive strips to determine a vehicle's direction of travel.
- Built-in gate and optional pop-up barriers, both supported by the lane controller
- Truck- or trailer-mounted control center so guards can be located remotely from the ACP

For locations that require higher levels of authentication and security, additional devices ensure that ID card authentication, biometric device authentication, or video camera inspection are automated. These processes can be designed to increase speed, or the process can be slowed for maximum security.

System Automation and Guard Security

For the most efficient operation with the highest levels of security, secure ACPs require system automation with guard overrides. In a fully automatic system, guard action is required only in the event of an alarm state. In a semi-automatic system, guard confirmation is required for each entry event.

A fully automatic system permits automatic access if all authentication criteria are met. For example, if the vehicle tag and card reader (and, if applicable, handheld or mounted biometric device) confirm the access right of the vehicle and its occupants, access points open automatically without guard intervention.

A semi-automatic system does not allow automatic access under any conditions. A guard must verify that a vehicle and its passengers are authorized to enter. Even if electronic systems confirm that a vehicle and its passengers meet all authorization criteria, a guard must still authorize access manually.

If the vehicle tag and card reader (and, if applicable, biometric device) fail to authenticate and deny entry, the system enters an alarm state. Alarm states can be customized for a variety of conditions in addition to authentication failures. For example, if lane devices are present, alarm states can be triggered if a vehicle attempts to enter the wrong way (against traffic flow) or a vehicle stays too long in a specific zone.

To increase guard security, the guard is located remotely from the ACP at a secure control center. The guard performs inspection with remotely operated video cameras. A driver camera identifies the driver of the vehicle against an authorized photograph stored in the database. Other types of cameras may include vehicle inspection cameras that allow multiple views of the vehicle and special remote tracking cameras, which have the capability to monitor unusual activity in their field of view.

Access Control Devices and Software

A secure ACP system requires lane hardware and software to route vehicles, to coordinate information collection, to assess vehicle and driver authentication, and to permit or deny access.

In a secure ACP, the lane controller coordinates input from authentication devices and traffic control devices. The authentication devices include video cameras, tag readers, card readers and biometric devices. The traffic control devices include gates, barriers, and signage. After collecting data from all input devices, the lane controller transmits the data to an interface monitor that can be controlled from near the access point or from a central location. In an automatic system, the lane controller can then authorize the traffic control devices to allow a vehicle to enter. In a semi-automatic system, guard confirmation is required.

At the center of the authorization process is a software application with a database of authentication data and a graphical user interface. The software maintains a database of authentication data and assembles the information collected at the ACP for review against stored data. The database manages personal information on the individual, photo, vehicle information, and other forms of identification including other ID cards and biometrics. The software coordinates a lane status monitor, multiple video camera feeds, and a guard interface environment that can be monitored and controlled from a central location.

The final function of the software is to provide analyses of control point activities. These include alarm tracking and reports on guard overrides.

Conclusion

A trailer-mounted RapDAC system allows rapid deployment, and more robust authentication and traffic control options are available for more dangerous locations. The system can help keep security forces out of harm should a suicide bomber attempt to crash a gate or slip past a checkpoint. The varying security needs of individual ACPs can be addressed by customizing RapDAC installations, but the technology requirements are similar.