

If only they'd had a driver-based security system.



Top 5 Things you should know about Automated Vehicle Perimeter Security Access

1 Know WHO is at the gate

- A. Identifying the vehicle by an attached Radio Frequency Identification (RFID) device rather than the driver credential could encourage a perpetrator to steal a vehicle to use for access to your facilities, making the vehicle a "Trojan Horse" by giving automated access to what is perceived as a safe entity.
- B. Another "Trojan Horse" can be created by copying common key fob transmitter code into the memory of a built-in gate activation reader/transmitter (found in any number of passenger vehicles), thus creating duplicate identities from the one authorized device.
- C. In the optimal security scenario, you should be able to automatically identify both the driver and the vehicle by separate credentials and be able to assign specific valid drivers to specific valid vehicles, without the risk of having the credential(s) be copied. You also want to make sure such a device is automatically disabled once the driver credential is removed.

2 Eliminate potential attack points

- A. Requiring a driver to stop, roll down the window and present a card or punch in a key code represents a major vulnerability in your security system as a potential attack point.
- B. The earlier automated identification can be established by the reader on the perimeter, the more time the back-end system will have to process, validate ID and safely get the gate out of the way of the approaching vehicle to eliminate the need to stop at the gate.

3 Accurately establish what your automated system identifies and WHERE

- A. Sometimes you can have too much of a good thing. This is particularly true with Long Range omni-directional RFID systems, such as key fob transmitters. The nature of omni-directional technology will allow you to identify vehicles at very long ranges. However, it will not be able to identify where it is in relation to the gate other than within a certain radius of your gate on either side.
- B. A better solution is a directional, adjustable reader with the ability to focus on one vehicle/driver at a time in each lane as they approach the gate. With this type of technology, the need for add-on components such as ground loops, etc. will be eliminated. This will result in higher read reliability, better system performance and lower installation costs.

4 Make automated vehicle access reliable, convenient and safe for the users

- A. Traditional pedestals required for short range card access readers and keypads present a dangerous obstacle in the roadway. They also present a challenge to drivers in different size vehicles trying to reach them from the interior of the vehicle—often resulting in damage to vehicles and equipment.
- B. Long Range Automated Vehicle Access readers eliminate this obstacle by being mounted out of the way, thus enabling unencumbered access for vehicles of all sizes from the smallest compact car to the largest truck.
- C. Accurate Long Range Vehicle Identification is accomplished through the use of an active battery powered tag. By being internally powered, the tag does not need to be "powered up" by the reader. Unlike passive nonpowered tags, the active tag is constantly "awake" and ready to reflect its ID number at very low reader power emission levels. The active tag system yields consistent accurate reads at distances up to 10 times that of common passive systems. Battery life in an active tag should yield 5–8 years of service.

5 Reduce cost of ownership

- A. When evaluating the cost of implementing automated vehicle access, it is important to clearly identify all associated costs and not just the cost of the tags and readers.
- B. Complete cost of ownership includes:
 - i. Any additional equipment required to accurately determine vehicle position, such as ground loops and additional relays.
 - ii. Any additional equipment required to interface with a standard security panel such as Wiegand converters, etc.
 - iii. Additional installation and maintenance costs of any required add-on components.
 - iv. Cost of replacement and frequency. For example, tags fixed permanently to the windshield will have to be changed every time a vehicle is replaced or the owner no longer is granted access. Assume a 20% tag replacement ratio per year and you will have repurchased all tags in your system in 5 years.
 - v. Ongoing service costs resulting from less than satisfactory operational reliability of inexpensive passive or omni-directional systems.

Contact Us: www.tuxen.us/nedapavi
Info-us@nedap.com
417-339-7368

nedap
Automatic Vehicle Identification