Vehicle Disabling Systems

Objective

Vehicle disabling systems are used to prevent unauthorized users from initially operating a vehicle and to gradually decelerate and stop a vehicle in-transit under certain pre-determined conditions.

These systems can be designed to be activated for specific situations, such as unauthorized access or use of a vehicle; loss of communication with a driver; discovery of security violations; vehicle entry into unauthorized areas; vehicle departure from predetermined routes; prevention of engine damage due to detected system failures; crisis or emergency situations; and mandatory maintenance needs.

Description

There are a number of types of vehicle disabling systems. Some utilize on-board electronics to immobilize the vehicle's engine or braking system to gradually decelerate a vehicle in transit or prevent its initial operation. Others can be engaged remotely using a combination of on-board computers integrated with wireless communications; or non-remotely, utilizing technologies that the driver, operator, or, in some instances, the vehicle itself could execute locally. The systems can be activated manually or automatically based on pre-programmed security conditions.

PROPANE TRUCK Driver Authorization systems

Remote vehicle disabling systems typically rely on a wireless communication system to provide their basic functionality. They can be integrated with panic buttons and on-board computers requiring user identification and/or password log-ins. For non-remote systems, a keypad or key-fob may be utilized as a part of these systems for arming, disarming, and controlling the security system at the asset itself. Non-remote manual systems can also involve the use of in-cab shut-off devices to other vehicle systems, such as electronic ignitions and air brakes.

Remote Vehicle Disabling Systems

Remote vehicle disabling systems provide authorized users at remote locations the ability to prevent an engine from starting, prevent movement of a vehicle, and to stop or slow an operating vehicle. Remote disabling allows a dispatcher or other authorized personnel to gradually decelerate a vehicle by downshifting, limiting the throttle capability, or bleeding air from the braking system from a remote location. Some of these systems provide advance notification to the driver that the vehicle disabling is about to occur. After stopping a vehicle, some systems will lock the vehicle's brakes or will not allow the vehicle's engine to be restarted within a certain timeframe.

Remote disabling systems can also be integrated into a remote panic and emergency notification system. In an emergency, a driver can send an emergency alert by pressing a panic button on the

Then, the carrier or other approved organization can be remotely alerted to allow a dispatcher or other authorized personnel to evaluate the situation, communicate with the driver, and/or potentially disable the vehicle.

Non-Remote Vehicle Disabling Systems

Non-remote vehicle disabling systems provide authorized users the ability to restrict or prevent vehicle operation in three ways: through the use of wireless technology when they are near the vehicle; through on-board actions by the driver/operator; or through a combination of both. Non-remote vehicle disabling systems include driver identification authentication technologies, tamper detection alerts, brake locks, and emergency notification panic buttons for disabling the truck in case of an emergency or other event.

A single sign-on module is utilized for driver authentication in order to initiate the operation of a vehicle. The driver uses passwords, pin numbers, or biometrics to start the vehicle and to access other on-board wireless communications applications. All activities related to the use of the vehicle are associated with the driver signed-in at the time. This information can be used for dispatch, driver performance, and driver log purposes.

Several different types of technologies can be used to non-remotely disable a vehicle. Panic buttons carried by the driver or within reach of the driver inside the vehicle can be activated to disable a vehicle or send out an emergency notification. Electronic ignition systems allow the driver to automatically activate the system when the key is removed from the ignition and reactivate the system when the key is replaced into the ignition. A relatively low-cost means of vehicle disabling is the utilization of a brake lock device to prevent the movement of the vehicle. A brake lock device shuts down the air line from the tractor to the air brakes in the tractor (and if hooked up, to the trailer). Release of the brake lock system is the only way to move the vehicle.

Application

Important components of vehicle disabling systems are hardware mechanisms that restrict vehicle use. Some are on-board computer technologies that identify the driver to allow authorized use while preventing unauthorized use. Others utilize mobile communication technologies that allow a remote dispatcher or other operator to communicate with the driver and/or the vehicle, and if necessary, activate the vehicle disabling system.

Driver authentication is a vital part of many vehicle disabling systems. Intelligent on-board computers can be utilized for driver identification through global login access where a driver enters login information into a cab-based interface. Similar to a username and password on a computer system, global login is an authentication feature of some wireless communications systems. Through the use of a driver login process, the login information (user ID and password) entered into the truck-based interface by the driver is verified by preset procedures both locally on the vehicle and over the air using the wireless communication system. If this verification fails, various configurable alerts and resulting actions can be triggered up to and including vehicle disabling with the aid of an on-board computer.

Other authentication technologies utilized in several vehicle disabling systems range from PIN number entry to biometric-based systems. The most common biometric-based technologies for

information on a biometric smart card carried by the driver, then the driver is verified and able to start the vehicle. If a match is not made, the vehicle cannot be started and the fleet dispatcher is typically notified of the failed attempt.

Vehicle disabling systems can be integrated with many on-board wireless communications systems that include other features, such as door sensors, cargo sensors, temperature sensors, electronic cargo seals, and trailer connection and disconnection systems. For example, if an on-board computer system detects a loss of signal from the communication network or tampering of electronic cargo seals, a pre-determined vehicle disabling protocol can be initiated.

Additional monitoring processes using on-board sensors that detect changes in load volume, door status, exposure to radiation, or temperature can a generate security alert notification that will trigger a vehicle disabling protocol. In vehicles that monitor trailer information, a vehicle disabling protocol can be prompted when a trailer has been disconnected from its assigned tractor or when a trailer door lock system has been violated.

Vehicle disabling protocols can also be activated by critical changes in the status of important vehicle systems. Since on-board computers monitor processes such as coolant temperature and engine oil pressure, a message can be sent to the driver and dispatcher about these conditions alerting them that systems are at unsafe levels. Then, a vehicle can be prevented from starting if unsafe system parameters are discovered prior to vehicle usage. Carriers with refrigerated units (reefers) are significant users of this feature.

Vehicle disabling can be utilized by authorized personnel with a wireless communication system's geo-fencing feature. Dispatchers or fleet operators can create a geo-fence or defined electronic boundary made up of geo-coded points for particular vehicles or routes. If a vehicle enters a restricted geo-fenced area, or exits the defined areas, the dispatcher or fleet operator can be alerted to take necessary actions to secure the vehicle. Currently, no systems have the capability of engaging automatic vehicle disablement for geo-fence violations.

Operations and Benefits

Depending on the actual vehicle disabling technologies utilized, fleet operators can have additional connectivity and communication with their drivers and vehicles compared with fleets not utilizing such technologies. When vehicle disabling systems are integrated with on-board communications and tracking systems, fleet managers can actively monitor security parameters, vehicle routes, performance, maintenance, and fuel usage?whether the vehicles are running locally or on a long-haul. These monitoring capabilities provide operational efficiency benefits for fleet management optimization by providing information about vehicle operation from origin to destination.

Vehicle disabling systems can improve secure operations of carriers who haul high-value or high-risk cargo, such as hazardous materials. Access can be limited to authorized drivers by dispatchers or fleet managers who can manage driver authentication codes and truck identifications, change codes over the air, and disable the vehicle, if necessary. To help prevent theft, a valid driver authentication code can be required before a vehicle can be started or moved. Also, if there is tampering with any integrated security device or fleet management system, the vehicle can be placed in a secure state and an alert can be sent over the air to the carrier. Carriers can also change driver authentication codes and secure a vehicle if a driver suddenly leaves the company, but still has access to the vehicle. The capability to disable the vehicle over the air is also available if dispatchers become

aware of a stolen or hijacked vehicle. Even if a truck is moving, the vehicle's speed can be gradually reduced to allow the vehicle to be brought to a safe and controlled stop.

Technologies, such as ignition locks and brake locks can also be used to minimize vehicle theft by prohibiting vehicle movement. These security devices are permanently installed in the vehicle, and they must be utilized in order to operate the vehicle.

Cost

The cost of vehicle disabling systems depends upon the type of system installed (i.e., a simple on-board system versus a multi-functional system), the number of systems purchased, and the type of installation required.

The costs for less complex on-board systems (such as an ignition lock or brake lock) range from under $100 to over $300 per unit, plus installation costs. Installation for these units could be done by a local technician.

The costs for basic, non-wireless driver authentication systems utilizing keypad entry range from approximately $500 to $700 per vehicle, plus installation costs. Installation for some of these units could be completed by a local technician.

The costs for systems integrated with on-board wireless communications and multi-functional features range from approximately $2,000 to over $3,000 per vehicle, plus installation costs. Installation for some of these systems can be completed by a trained technician who is familiar with the technology. However, for technical and/or security reasons, some systems require manufacturer installation only.

In addition to installation costs, some vehicle disabling systems (especially remote monitoring systems) may also require a monthly fee for maintenance and monitoring.

Vendors

Systems Providing Remote Disabling

AirIQ, Inc. Product: OnBoard™ 1099 Kingston Road, Suite 233 Pickering, ON, Canada L1V 1B5 Phone: 905-831-6444 Toll Free: 888-606-6444 http://www.airiq.com	**GPS Management Systems** Product: Asset Tracking 480 E. Northfield Drive, Suite 500 Brownsburg, IN 46112 Phone: 800-914-8247 Fax: 317-852-0742 http://www.gpsmanagement.com
Magtec Products (USA), Inc. Product: M5K 871 Coronado Center Drive, #200 Henderson, NV 89052 Phone: 888-624-8320 E-mail: info@magtecproducts.com http://www.magtecproducts.com	**QUALCOMM Incorporated** Product: Vehicle Command & Control 5775 Morehouse Drive San Diego, CA 92121-1714 Phone: 858-587-1121 http://www.qualcomm.com
Safefreight Technology (USA), Inc. Product: SmartFleet™ 8000 N.E. Parkway Drive, Suite 200	**Satellite Security Systems, Inc. (S3)** Product: GlobalGuard 6779 Mesa Ridge Road, Suite 100

Vancouver, WA 98662 Phone: 360-256-1280 Fax: 360-397-0167 http://www.safefreight.com	San Diego, CA 92121 Phone: 858-638-9700 http://www.satsecurity.com

Systems Providing Non-Remote Disabling

BASE Engineering, Inc. Product: Driver Authorization System™ 1714 Rothesay Road Saint John, New Brunswick Canada E2H 214 Phone: 800-924-1010 http://www.baseng.com/products/DASsystems.html	**CGM Applied Security Technologies, Inc.** Product: TS4A Tractor Brake Lock 24156 Yacht Club Blvd. Punta Gorda, FL 33955 Phone: 941-575-0243 Fax: 941-575-0971 http://www.cgmsecuritysolutions.com

Disclaimer

The information provided in these guides about products and services available from private entities does not constitute an endorsement by the Federal Motor Carrier Safety Administration (FMCSA) of the views expressed by any non-Federal entity, or its products or services. FMCSA is publishing lists of vendors on this site solely in an effort to further public awareness of vendors identified as possible contacts for further information and possible purchase of different types of safety and security equipment. The list of vendors is not a complete list. The information in these product guides is disseminated by FMCSA in the interest of information exchange. The United States Government assumes no liability for the contents or use of these guides. These guides do not constitute standards, specifications, or regulations, and FMCSA provides no assurance that the listed vendors and their products and services meet applicable standards, specifications, or regulations. Links to Web sites outside the U.S. Government or the use of trade, firm, or corporation names within FMCSA's Web site are solely for the convenience of the user. Users who select a link to a non-government Web site leave the FMCSA Web site, and are subject to the privacy and security policies of the owners/sponsors of those Web sites. FMCSA does not control or guarantee the accuracy, relevance, timeliness, or completeness of information on a linked non-government Web site. FMCSA cannot authorize the use of copyrighted materials contained in linked Web sites. Users must request such authorization from the sponsor of the linked Web site. FMCSA is not responsible for transmissions users receive from linked Web sites. FMCSA does not guarantee that outside Web sites comply with Section 508 (accessibility requirements) of the Rehabilitation Act.