Physical Security in Railroad Intermodal Terminals

Carl R. Ball
James W. Rusteberg
Santa Fe Railway
Chicago, Illinois

A corporate commitment to good security is vital in preventing thefts of containers, trailers, and lading from railway intermodal terminals. The mobility of trailers, their relatively high value, and the significant volume transported by rail make them lucrative targets for thieves often associated with organized crime. Thefts that occur at intermodal terminals can represent corporate losses in the hundreds of thousands and sometimes millions of dollars. Security at intermodal terminals tends to be reactive to current criminal activity, rather than proactive or preventive. To obtain optimum crime prevention, design engineers and operating managers need to consider security a high or main priority in planning and operating the intermodal facility. Physical design and daily operating procedures can significantly deter crime. The security of intermodal terminals should include several broad factors such as psychological deterrence, physical security measures, and procedural checks and balances. Although the focus of this paper is on railroad intermodal terminals, the same principles of security are applicable to other types of intermodal facilities.

The focus of this paper is on railroad intermodal security at terminal facilities; however, the same principles are applicable to other types of terminals.

The implementation of strong security measures at intermodal terminals is a good, sound business investment. Thefts of trailers and containers now constitute one of the most costly casualty losses at terminals (Figure 1). The current consolidation of operations has resulted in a decrease in the number of intermodal facilities (2). Remaining terminals are being expanded beyond their original design and capacity. This creates physical security and operational problems far greater than ever anticipated. As a result, the transportation industry is just beginning to understand the potential dollar losses associated with inadequate physical security.

Crime prevention is a primary mission of all law enforcement agencies, and it also should be a major consideration in any business. Research on deterrence attempts to estimate the number of criminal acts not committed because of potential offenders' fear of apprehension and punishment. A basic understanding of psychological deterrence can assist in planning the physical design of terminals and in the implementation of operational procedures and security strategies (3).

The supression of crime by deterrence is a complex issue. General deterrence is the prevention of criminal behavior because of the perceived risk of criminal sanctions. Even though relatively few offenses result in arrest, prosecution, and conviction, general deterrence is the first and most logical approach to crime prevention (3).

From a corporate security standpoint, it is far less costly to prevent a crime than to investigate a crime after it has occurred. From a business perspective, there are a number of aggregate losses associated with the theft of a trailer or container. First is the loss of the trailer itself, usually valued between $10,00 and $40,000. Second, cargo stolen can cost as much as a $1 million. Third is the corporate cost to investigate the crime, which can range upward to $20,000 or more per incident. Not to be forgetten are the losses resulting from a dissatisfied customer whose shipment is stolen and illegally distributed. This may result in the shipper choosing an alternative transportation mode for future shipments, causing a decrease in sales and profits for the carrier.

In planning for physical security at intermodal terminals, a study of past incidents must be considered. This information is valuable in determining the degree of deterrence necessary. Potential offenders will likely have an accurate perception of the actual risk of detection and may be attracted to targets that rely heavily on "cosmetic" security. Recognizing the distinct difference between actual and perceived risk can help in assessing the potential for crime and provide a basis for planning physical security (4).

SECURITY SURVEY

The security survey is the first step in defining "risk analysis" perimeters at intermodal terminals. It is the most important technique in planning and implementing effective crime prevention measures. The major considerations in this process are the ability to assess the current and future crime potential and to develop practical, cost-effective preventive measures. This process can be completed in an organized manner with the cooperation of terminal managers, operations supervisors, and security planners. Their coordination is essential to ensure that all aspects of management philosophy and terminal operations are reviewed before physical security measures are made final and implemented (4).

Another major factor to consider at the terminal is the potential for loss. Obviously the greater the potential loss, the higher the degree of security that should be considered and implemented. These factors will have a significant impact on the funds budgeted for physical security.

An in-depth analysis of the intermodal terminal's security risks should point out excesses of protection as well as deficiencies. This may lead to cost savings and a more efficient and safe operation (4).

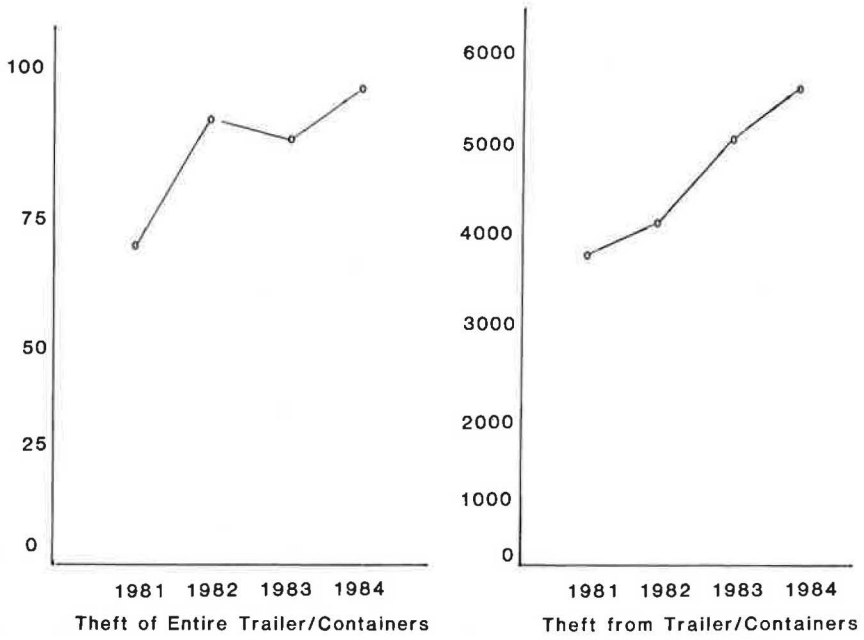

FIGURE 1 Incidents reported to the AAR, Police and Security Section *(1)*.

Before conducting a physical security survey it is important to meet with representatives of the various departments to discuss the terminal business philosophy, operations, and past incidents of criminal activity. This discussion should include any proposed terminal expansion and future business projections.

It also is important to survey other intermodal terminals within the general geographic area to analyze their successful security measures and history of criminal activity.

The rationale for physical security is based on a number of variables at each terminal. Hence, it is difficult to plan for every possible risk at a given site. No two terminals are exactly alike, and recommendations will vary depending on the unique geographic and operational features of the terminal.

The survey encompasses five basic aspects that become the foundation for a working format: (a) anticipation, (b) recognition, (c) appraisal, (d) opportunity, and (e) planning (4).

Anticipation is simply part of planning ahead by assessing current conditions. Security planners are capable of recognizing conditions that constitute a crime risk. This, in turn, leads to an appraisal of the degree of risk. In evaluating the conditions, the security survey must consider the opportunities for crime including potential security breaches and operational weaknesses. Finally, the planning phase includes analysis of security equipment, formal written proposals, and budget submissions (4).

The following questions should be answered in conducting a physical security survey of any intermodal terminal.

1. What kinds of lading are shipped through this terminal and what is the potential dollar loss for a single incident?
2. What are the natural barriers in and around this terminal?
3. What has been the history of crime and dollar loss at this terminal?
4. What types of crime and losses occur at other intermodal terminals in the general geographic area?
5. Can this terminal be designed to have the checkpoint located at the exit gate?
6. Can existing personnel be used to accomplish the operational and security objectives?

PERIMETER BARRIERS

The fundamental principles of perimeter protection have not changed in decades. The need to delineate and enforce property boundaries is basic to sound physical security. When planning perimeter protection at intermodal terminals, several interrelated factors must be considered. Foremost is the need to assess accurately the degree of protection at a particular terminal. Security fencing serves not only to delineate boundaries but to control entry and exit from terminals, deter intruders, and detect trespassers.

Security perimeter barriers differ depending on location, geography, and purpose. Barrier specifications need to be reviewed at each facility to ensure compliance with local building codes and conditions that affect construction. The latter requirement must take into consideration the climate and terrain. It is important to assess accurately the philosophy of those who ultimately are responsible for the administration, operation, and maintenance of the terminal when considering the type of perimeter fencing installed.

Some barriers are opaque, others do not obstruct vision. Opaque barriers include brick or block walls, boards, or anything that restricts the view. These maintain privacy so thieves are not attracted to the terminal by viewing trailer locations or contents. See-through fencing such as chain link enables terminal employees and security personnel to keep trailers and containers under surveillance.

The many kinds of fencing available can also be divided according to their primary function: (a) boundary fencing, designed to delineate a boundary; (b) barrier fencing, intended to obstruct entry; (c) safety fencing, designed primarily to meet a statutory or other safety requirement; and (d) security fencing, designed to keep out intruders.

Perimeter fences should be protected by interior guardrails to prevent vehicles backing into them. Guardrails also prevent thieves from driving through the fence.

Effective security fencing needs to be of sufficient height, usually 8 ft, and enhanced with barbed wire or razor ribbon on top. Posts should be set in concrete to prevent movement. Chain link fencing is the most common barrier in perimeter protection. The landscape, vegetation, terrain, and environmental conditions, to a large extent, will determine the need for fencing or if natural barriers or some other protection will suffice. In addition, high-security areas should have the fence equipped with motion detection sensors. Fence sensors fall into two general categories, electromechanical and electronic.

ELECTRONIC ATTRIBUTES

Considering the size and number of intermodal terminals on most railroads, the addition of inspection, dispatch, or railway security personnel at each terminal is the most costly approach. Additional personnel are not necessarily the most effective way to prevent crime.

Security goals should be translated into a systems-intensive environment (5). Electronic attributes can extend existing dispatch and security capabilities by monitoring remote entrances, exits, and strategic locations from a central location.

Electronic security systems provide support in four general areas:

1. Closed-circuit television equipped with videotape recording and motion detection capabilities gives fewer personnel the ability to monitor numerous locations simultaneously. Not only are fewer personnel needed, but videotapes serve as evidence in the event of a crime. The motion detection enhancement provides remote alarm monitoring of multiple points from a single location.
2. Intercommunications (radio, telephone, loudspeaker, or intercom) extend the aural sense.
3. Intrusion detection devices that monitor perimeters eliminate the need for constant human surveillance.
4. Access control systems at terminal entrances and exits, employee gates, and other doors permit remote control of several points.

Even with these four physical security concepts, protection of each terminal entrance requires people, be they inspection, dispatch, or security personnel (6). With the electronic equipment described, the need for additional personnel with separate functions is reduced with each application and security enhancement.

In some unique applications electronic monitoring and video recording may be all that is necessary for adequate security. In other applications, a combination of electronic monitoring and personnel, along with strict operational procedures, may provide adequate protection.

CLOSED-CIRCUIT TELEVISION

Closed-circuit television (CCTV) has become a common security measure to augment dispatch and security personnel. CCTV is an extension of the human eye. It monitors events as they occur, in contrast to film cameras that record past events. CCTV is an accepted management tool in the protection of people and corporate assets. Applications at intermodal terminals are limited only by the imagination.

Features available on cameras today can increase the operational efficiency of the system. One motorized camera with pan, tilt, and zoom capabilities may be far more efficient and effective than three or four stationary cameras. A split screen generator puts images from two cameras onto one monitor.

CCTV can be used to view and record identifying numbers of tractors, trailers, and drivers for security purposes; and it can be used to discover vehicle damage. As an administrative tool, CCTV can aid in conducting work-related time studies and other business applications.

Video cameras can be equipped with sequential alarm switchers that switch from camera to camera with variable dwell times. When the alarm switch detects an intrusion, the sensor automatically shifts to the nearest camera and turns on a videotape recorder. The time and date are also recorded on the tape.

One of the best applications at intermodal terminals is the use of so-called "smart cameras." The term applies to the memory capability of the microprocessor control. The memory unit is programmed to react to changes in the image (i.e., motion detection) within the camera's view. Thus the system is able to distinguish between moving and stationary objects (6).

With a recorder, CCTV becomes not just an observation system but an evidence system, recording invaluable information for investigation and prosecution. New applications include solid-state storage and freeze-frame encoding of multiple pictures from several cameras simultaneously on one videotape.

Creative uses of CCTV and its success in deterring crime have changed the video camera from an Orwellian image of ultimate control into a familiar, even comforting, sight (7). A closed-circuit television system is no panacea for controlling all crime. The motivation and need for CCTV become obvious after an incident that results in a large financial loss. Managers then can see the need for a remote "set of eyes" that can watch several physically disparate locations from one monitoring point. The diverse range of cameras, monitors, tape recorders, and other accessories available in CCTV today means users can assemble a system that will do precisely what they want it to do. Also, new applications for the equipment may be added after installation.

INTRUSION DETECTION DEVICES

A fence is merely the first line of defense in perimeter security. Intrusion detection equipment used in conjunction with perimeter fences can enhance security by adding another dimension (Figure 2). Detection devices sense the presence of objects or people within a given area.

There are numerous types of devices. They can be mounted directly on or next to fences or installed within a corridor area. If corridors are left next to perimeter fences, detection equipment can monitor these areas electronically and provide an audible alarm at the terminal checkpoint. Personnel need respond only when an alarm is sounded. This equipment can be enhanced with a panel containing zone lights that provide checkpoint personnel with a graphic display of the location where the fence or corridor is breached.

Consideration should be given to systems with two or more sensing capabilities; for example, buried cables combined with above-ground microwave sensors. Buried cable devices detect changes in ground pressure or in the ground's magnetic field caused by people or objects standing on or passing over buried transducers.

Fence sensor technology has often been criticized because it is defeatable by a knowledgeable intruder. Underground perimeter protection is virtually invisible and less prone to attack.

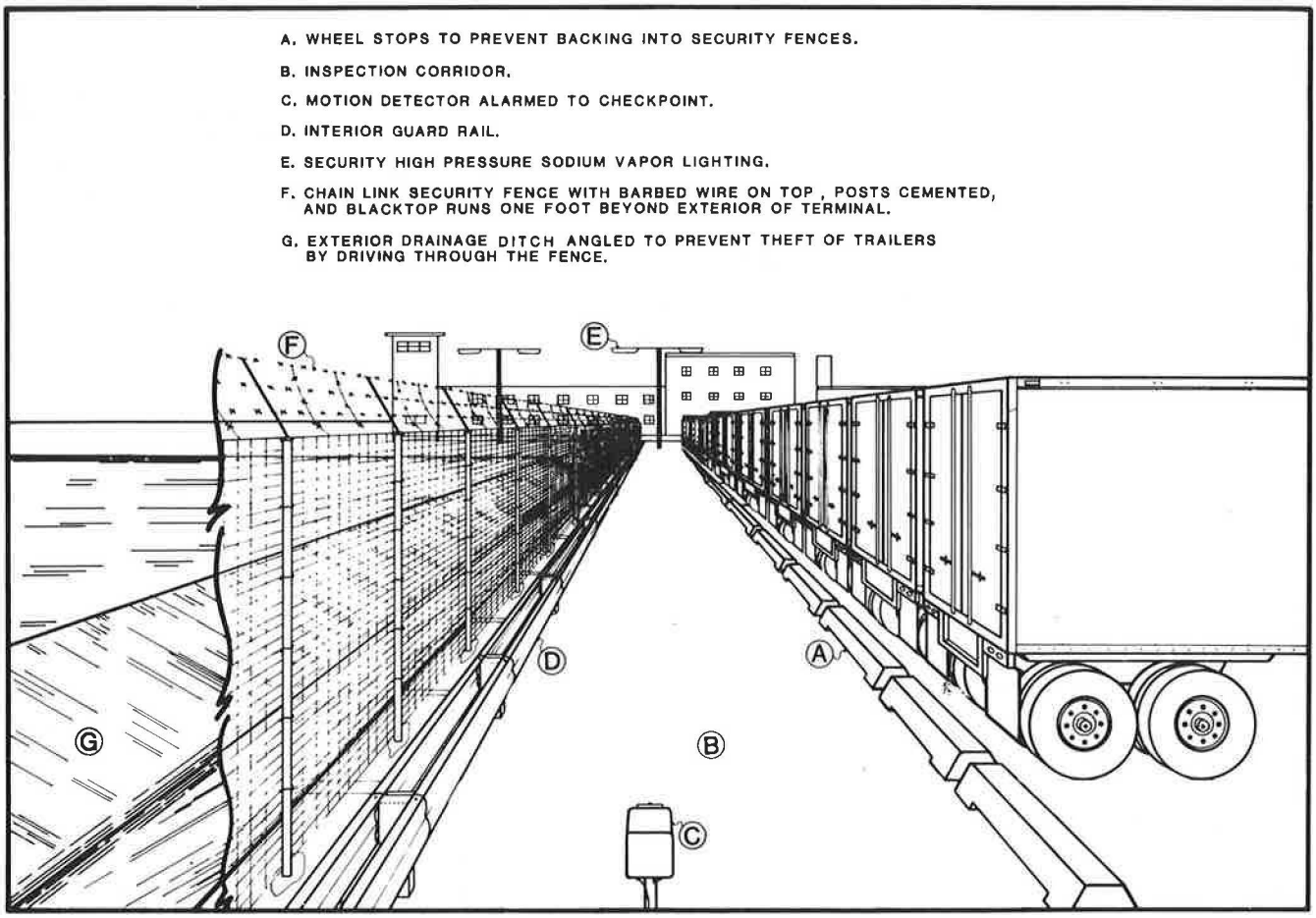

FIGURE 2 Perimeter security.

SECURITY LIGHTING

Good lighting is a strong deterrent to crime. Perimeter lighting should include areas on both sides of fences and guardrails and within corridors. High-pressure sodium vapor lighting, with its distinctive bright yellow color, has proven efficient and effective in security applications. It provides more than twice the luminaires of the standard mercury vapor and is more cost efficient.

It is important to have adequate lighting at terminal entrances and exits. When planning lighting, the main consideration is to provide variations in lighting between the terminal buildings, trailers and containers, and perimeter areas. Lighting at terminal exits must be located behind camera locations to avoid silhouetting the subject and to enhance video resolution.

Security lighting gives terminal supervisors and security officers the ability to maintain a high level of security at night and observe activities around trailers and inside terminals. It should provide even illumination on areas bordering the terminal and focus light in the direction of potential intruders. In general, lighting should be directed downward, bathing the terminal property in overlapping patterns with as few shadows as possible.

OTHER PHYSICAL SECURITY MEASURES

There are a number of physical security measures and procedures that enhance security at intermodal terminals. One measure often overlooked is the use of natural barriers. Exterior drainage ditches, for example, can serve as a natural security barrier. Properly planned, these ditches can prevent a thief from driving through the fence and off the property.

It is important from a security viewpoint that terminal entrances and exits and trailer and container locations be properly marked with signs to direct drivers within a terminal. Routing traffic in a single direction not only enhances operations and safety but aids in security efforts.

Spring-loaded road spikes can aid in controlling the traffic flow and prevent unauthorized entry or exit from terminals (Figure 3). One disadvantage is that they can be compromised with wood blocks, allowing a truck to drive over the spikes without puncturing the tires. Safety factors also should be considered. Spikes may freeze in ice and snow, causing undesired tire punctures. This problem can be overcome with heating elements to prevent malfunctions.

SECURITY DISPATCH PROCEDURES

The following list contains various security dispatch procedures and guidelines.

1. Inspection and dispatch forms should be numbered sequentially and kept in a secure location.
2. Inspection and dispatch forms should include the drayage contractor's name, the truck driver's state driver's license number, and the tractor's state license plate number or numbers.
3. A computerized list of authorized drayage

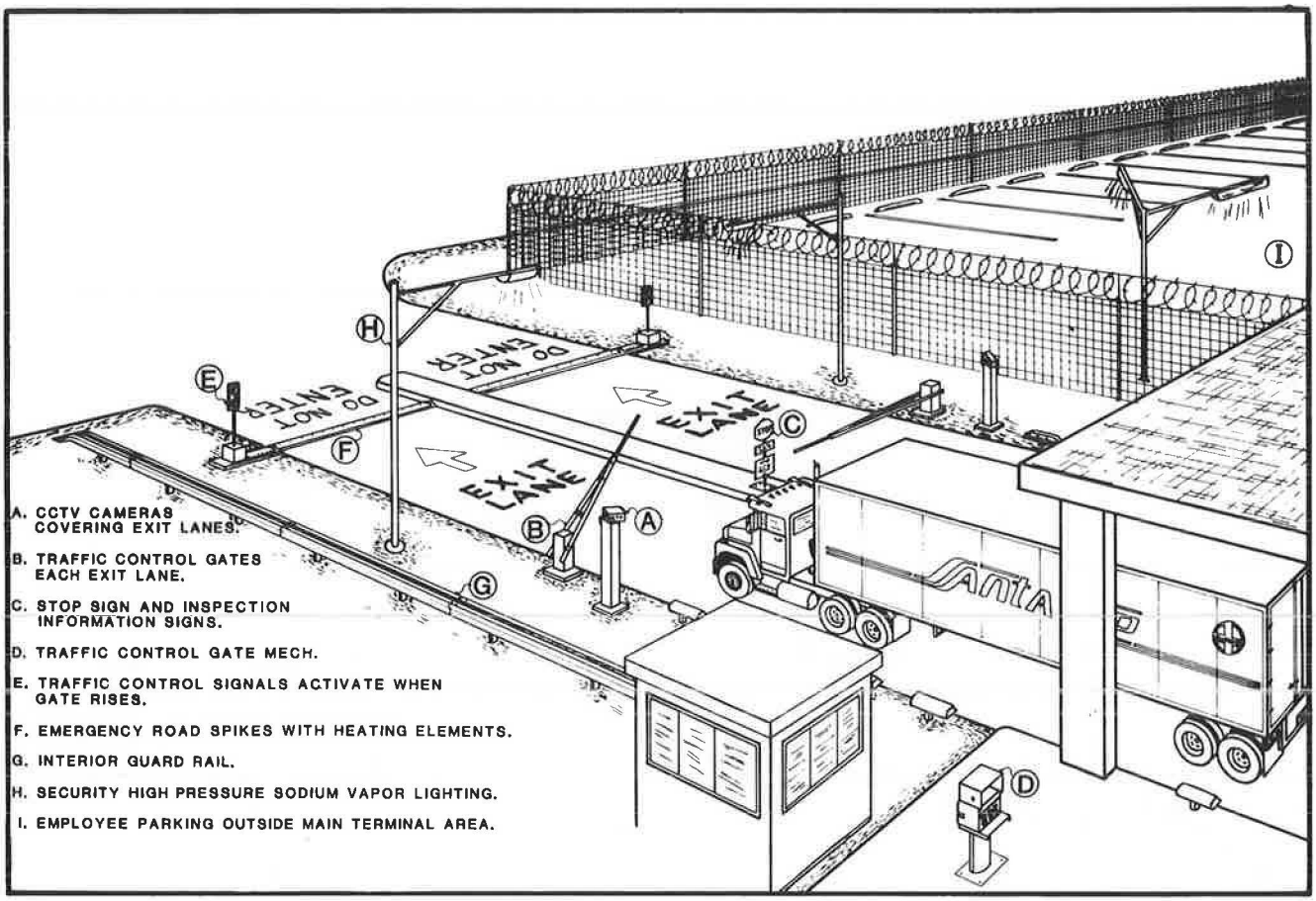

FIGURE 3 Exit gate security.

contractors and their drivers, including pertinent information on all drivers, should be maintained and updated.

4. Truck drivers unable to produce a valid driver's license should be required to produce two other forms of verifiable identification. In addition, the drayage firm should be contacted and the driver's authority verified before departure from the terminal.

5. The truck driver's signature should be legible and, if not, he must print his name clearly next to the signature.

6. Inspection and dispatch forms should be reviewed for all required information, and the trailer and container initials and numbers should be verified before departure is permitted.

Good security dispatch procedures can have a significant impact on terminal crime prevention. Documents used in the inspection and dispatching of trailers and containers should be sequentially numbered and kept in a secure location. It is important from a security perspective that they be issued sequentially. A stolen document used out of sequence will alert checkpoint personnel to a possible theft or abuse of dispatch procedures.

It is also important to hold dispatch personnel responsible for the security and proper issuance of such documents. Employees who issue the documents directly to truck drivers must review them for complete and accurate information. It is extremely important that the trailer initials and numbers be visually verified and compared with the inspection and dispatch form. In addition, seals on the rear or side doors, or both, should be examined and physically tested to ensure their integrity and proper placement through door hasps. This information must be noted on the inspection and dispatch form including the initial and number of any and all seals. Cargo security seals should be used on high-value shipments.

Signatures of truck drivers must be legible on inspection and dispatch forms. Dispatch personnel should require printing of the truck driver's name next to any illegible signature. The driver's license number of the truck driver and the tractor license plate number should also be noted on the inspection and dispatch form. This includes the state where issued. Truck drivers unable to produce a valid driver's license should be required to produce two other verifiable forms of identification. In such cases, the drayage contractor should also be contacted and the driver's authority verified before departure from the terminal is allowed.

Names, addresses, and telephone numbers of all authorized drayage contractors and their authorized drivers should be kept at terminals for verification of information. Security personnel have found that computerizing information on drayage contractors, drivers, tractor descriptions, licenses, and so forth is invaluable as a security procedure and for investigative purposes in the event of theft.

Rules governing dispatch procedures and conduct of drivers while at intermodal terminals should be established and posted in a conspicuous location, advising them of the policy requiring verifiable information.

Special, dual-lens identification cameras are used in many terminals to simultaneously photograph inspection and dispatch forms, truck drivers, their

driver's license, and the date and time of each transaction. Designed specifically for this function, these cameras provide valuable photographic evidence in the event of a vehicle theft or if one has been taken in error. Dual-lens identification cameras are a strong deterrent to theft.

CONCLUSION

Personnel operating intermodal terminals are faced with increasing crime on one hand and static or diminished resources on the other. They are struggling with budgets that have been reduced by administrative cuts or inflation, or both, while security requirements have increased.

The following list is a summary of various intermodal terminal physical security measures. It is the responsibility of engineers, terminal managers, and security planners to develop and implement reasonable, cost effective, physical security measures to eliminate and minimize costly thefts.

1. A terminal should have one entrance and one exit, and they should be located together.
2. The dispatcher's office and security checkpoint should be located together between the inbound and the outbound lanes. The interior should be divided by a wall that keeps personnel and functions separate. All traffic should pass this location to enter or exit the terminal.
3. Personnel parking should be located outside the facility with a separate vehicle entrance gate.
4. The entire facility should be enclosed by an 8-ft chain link fence with barbed wire or razor ribbon on top. Barbed wire should be placed at a 45-degree angle toward the exterior of the fence.
5. Guardrails should be placed around the interior of the fence line to prevent vehicles from being driven through the fence. Wheel blocks should be installed to create an adequate corridor for security inspection of the fence perimeter.
6. Rail leads entering the facility should be controlled by electronically activated sliding gates. These gates should be controlled by the operations supervisor, and an alarm should sound at the security checkpoint when the gates are opened.
7. Electronically controlled gates should be located at each exit lane to prevent trucks from leaving the facility unnoticed or unauthorized.
8. Red and green traffic control signals should govern each exit lane and be controlled by checkpoint personnel.
9. Electronically operated road spikes should control outbound truck lane usage. The spikes should be equipped with heating elements when used in cold climates. Security officers should be able to activate outbound spikes should a driver attempt to "run" the gate with a stolen trailer.
10. Closed-circuit television cameras with videotape recorders and monitors should be used to record vehicle movement at exit lanes and throughout the terminal. Cameras should be enclosed in environmental housings and located on 40-ft towers. They should have pan, tilt, and zoom lens capabilities. Exit lane cameras should be located to record the front of tractors (including license plates and other identification numbers), drivers' profiles, and the side markings and numbers on trailers and containers.
11. The dispatcher's office should be equipped with dual-lens identification cameras to photograph the driver, his driver's license, and the dispatch form. The dispatch form must contain all information and indicate the date and time each trailer was removed from the terminal.
12. Drivers should be provided with a prearranged code to remove any trailer from the facility. The code should be supplied by the intermodal supervisor to the consignee. The consignee provides the code to the drayage firm that in turn supplies it to the driver for authority to remove a trailer.
13. The facility should be illuminated with clusters of high-pressure sodium vapor lights on 80-ft towers, with additional lighting at the entrance and exit lanes.
14. Wide corridors should be left around the interior of the perimeter fencing and motion detection systems installed to detect intruders.
15. All brush and trees should be removed from around the fence perimeter.

Security planners have found that crime prevention training for terminal personnel through meetings, literature, and security surveys also helps to reduce crime. An effective security consciousness crime prevention program can be an important element in meeting terminal security needs. Crime prevention programs and physical security measures can prevent crimes that would require the work of many investigators to solve.

The implementation of physical security measures capitalizes on the concept of manpower leverage, thus obtaining a comparatively large result through a process that amplifies the efforts of a systems-intensive environment (5).

There is no single, all-inclusive, physical security tactic to prevent all crime. Variations of the systems described in these guidelines, designed for the specific needs of terminal operations, will greatly enhance crime prevention efforts. The implementation of security measures that are perceived by thieves as valid psychological deterrences, along with adequate procedural checks and balances, will significantly reduce the risk of crime at intermodal terminals.

The effectiveness of any security system or procedure is only as good as its weakest link.

REFERENCES

1. Annual Statistics on Crimes Against Railroads. Association of American Railroads, Washington, D.C., Police and Security Section, 1981, 1982, 1983, 1984.
2. R. Roberts. Defining the Intermodal Terminal. Modern Railroads, Vol. 39, No. 7, July 1984.
3. J.J. Collins. Can Criminologists Measure Deterrence? Security Management, Vol. 27, No. 6, June 1983.
4. J.F. Broder. Risk Analysis and the Security Survey. Butterworth Publishers, Inc., Reading, Mass., 1984.
5. C.L. Cronkhite. Crime Prevention from an Administrative View. Journal of California Law Enforcement, Vol. 15, No. 2, Spring 1981.
6. W.N. Hershfield. The Staff/Equipment Balance. Security World, Vol. 21, No. 6, June 1984.
7. L.S. Jones. Cargo Security. Butterworth Publishers, Inc., Reading, Mass., 1983.