

CONF-961113--R

SAND96-2730C
SAND--96-2730C

Perimeter security for Minnesota correctional facilities

David Crist
Acting Assistant Commissioner-Institutions
Minnesota Department of Corrections
1450 Energy Park Drive
St. Paul, Minnesota 55108

RECEIVED

NOV 26 1996

OSTI

Debra D. Spencer
Sandia National Laboratories
Albuquerque, New Mexico 87185-5800

KEYWORDS: perimeter security; corrections; correctional facility; prison; perimeter design; security.

Abstract

For the past few years, the Minnesota Department of Corrections, assisted by Sandia National Laboratories, has developed a set of standards for perimeter security at medium, close, and maximum custody correctional facilities in the state. During this process, the threat to perimeter security was examined and concepts about correctional perimeter security were developed. This presentation and paper will review the outcomes of this effort, some of the lessons learned, and the concepts developed during this process and in the course of working with architects, engineers and construction firms as the state upgraded perimeter security at some facilities and planned new construction at other facilities.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

2. History

There are seven prisons in Minnesota, housing approximately 5000 adult felons. Seventy percent of all offenders are convicted of crimes against a person, including murder, rape, robbery, kidnapping and assault. There are four security classifications: maximum, close, medium and minimum.

Maximum security is reserved for offenders with the most violent crimes on the streets and whose behaviors in prison create concerns for the security and well-being of others. Offenders' movement within the facility is severely restricted and scheduled. They are housed one to a cell in living units of fifty-two men. The maximum facility is horseshoe shaped and the exterior of the horseshoe is earth bermed to the level of the roof. There is a taut wire system on the interior edge of the roof. The double perimeter fence is three hundred yards away and is equipped with razor ribbon and another perimeter detection device.

There are two close security facilities. Inmates still live one to a cell, but there is somewhat more freedom of movement within the prison. One of these facilities is over one hundred years old and is surrounded by the longest continuous granite wall in the world.

The other, the Minnesota Correctional Facility-Stillwater (MCF-STW), is an eighty-five year old prison located in the St. Croix Valley twenty miles east of the Twin Cities of Minneapolis and St. Paul. There are one million interior square feet, most of which is encircled by a 22 foot stone and cement wall topped with guard towers. Approximately one thousand three hundred close custody inmates are housed in single cells in living units of two hundred fifty. Cells are stacked four tiers high. Each tier is sixty-four cells long (approximately 520 feet). The largest living units are located in the main building of the institution.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

**Portions of this document may be illegible
in electronic image products. Images are
produced from the best available original
document.**

Work and program space are located in separate buildings within the walled structure. Inmates leave the main building and walk a distance of three city blocks to reach these program areas. The recreation yard is between the wall and the main building. The north boundary of the recreation yard is the wall. (Inmates use the wall for handball, which is probably the institution's most popular recreational activity.) All the work and program areas are within twenty feet of the wall and inmates must walk in these areas to complete their assignments.

There are three medium security prisons. Each perimeter is maximum security, but the interior configurations resemble college campuses. Inside, there is a great deal more freedom of movement, relatively speaking.

The Minnesota Correctional Facility-Lino Lakes has approximately one thousand medium custody inmates and is located twenty miles north of the Twin Cities. There are 11 living units, housing between 52 and 232 inmates each. The secure perimeter consists of two chain linked fences with several coils of razor ribbon between them. One of the fences has an intruder detection device. All security zones are monitored by camera. There is a residential neighborhood within three hundred yards of the west perimeter of the facility.

Recreation, program and work areas are ringed by housing units which are approximately two hundred feet from the fence. The area between the fence and the units is off limits to the inmates.

As offender populations continue to rise, it has become necessary to improve the perimeters of these two prisons by increasing lighting, camera coverage, detection and delays to escape. As budgets continue to decrease, it has become necessary to improve security with fewer staff. Thus, our turn to technology. However, to purchase technology, we must navigate the bureaucracy.

3. Bureaucracy

Before the bureaucracy will consider physical changes to a facility, we are required to conduct a predesign study, which includes simple drawings of the project and a cost analysis. This usually amounts to one percent of the cost of the total project. Agencies must generate funds for this activity internally.

In Minnesota, changes of this magnitude are considered capital improvements. Because of the cost of these changes, it is necessary to receive legislative appropriations. Such appropriations must be recommended by the House and Senate bonding committees, approved by each house of the legislature and signed into law by the governor.

Once done, a request for proposals is published in the state register. Respondents submit their proposals to an architectural review board, which is charged with equitably distributing the state's construction business. As architects scramble to submit their proposals, they develop partnerships with engineering and security consultants, to whom they can subcontract technical aspects of the projects. A short list of architects is developed and oral presentations are scheduled. Corrections project managers are present and are asked for input after all presentations have been made. However, the decision regarding the award of architecture and engineering is made solely by the board based on the perceived adequacy of the plans and the somewhat fuzzier concept of fair distribution of the state's business.

Planning begins in earnest with a series of meetings between the architects and corrections. To avoid economic inflation, there is considerable incentive to finish planning quickly and begin construction. The legislative appropriation cannot be exceeded and more money will not be paid for inflation as a result of late completion. However, if a construction company can complete planning and construction ahead of schedule quickly and save inflationary costs, they still are allowed to bill for the whole bid amount. Therefore, little time is allotted for test bed planning. Indeed, most designs turn out to be theoretical and debugging is conducted after construction, not before.

Then, another request for proposals is published in the state register calling for construction bids. A walk through with potential construction firms is conducted during which the project is explained. Sealed bids are submitted. Typically, the work is awarded to the low bidder. Construction may begin after the firm submits the required proofs of competency and insurance.

Finally, it is no small feat to conduct business on the grounds of a correctional facility. Workers must submit proof of negative TB tests and they are searched coming and going. Tools must be accounted for each night. Security must not be breached. Contractors typically inflate their bids of a correctional project by twenty percent to make up for nonproductive time.

4. Developing a Physical Security System (PPS)

The Minnesota Department of Corrections began working with Sandia National Laboratories in 1993 to develop standards for the design and construction of secure perimeters. Concepts which had been refined to protect sensitive nuclear materials were turned inside out. After all, the target (freedom) for an escapee is outside the secure perimeter of a prison, not inside the secure perimeter as would be the case in a nuclear installation.

The first step in the development of a PSS design is to determine the objectives of the security system. To formulate these objectives, the designer must:

1. characterize (understand) the facility operations and conditions,
2. define the threat, and
3. identify escape scenarios and other potential adversary targets.

Characterization of facility operations and conditions requires developing a thorough description of the facility itself which should include the location of the site boundary, building locations, building interior floor plans, and access points. A description of the procedures within the facility is also required, as well as identification of any existing physical security features. This information can be obtained from several sources, including staff interviews, facility design blueprints, departmental procedures, security post orders, and maintenance records.

Next, a threat definition for the facility must be made. Information must be collected to answer three questions about the adversary:

1. What class of adversary is to be considered?
2. What is the range of the adversary's tactics?
3. What are the adversary's capabilities?

In prisons, adversaries can be separated into four classes: inmates, insiders, outsiders, and outsiders in collusion with inmates or insiders. For each class of adversary, the full range of tactics—deceit, force, stealth, or any combination of these—should be considered. Deceit is the attempted defeat of a security system by using false authorization and identification; force is the overt, forcible attempt to overcome a security system, and stealth is the attempt to defeat the detection system and exit the facility covertly.

Important capabilities for the adversary include his knowledge of the PSS, his level of motivation, any skills that would be useful in an escape attempt, the speed with which the escape attempt is carried out, and his ability to obtain and carry tools and weapons. Since it is not generally possible to test and evaluate all possible capabilities of an unknown adversary, the designer and analyst must make assumptions. These assumptions can be based on published information about human performance and the tested vulnerabilities of physical security elements.

Finally, target identification should be performed for the facility. All credible escape scenarios should be considered, including the defeat or by-passing of security system components or barriers, breaching of structural features or use of facility features as climbing or bridging aids, use of force or stealth, or the defeat of procedures by deceitful means such as forged gate passes. The credibility of escape scenarios usually depends on identification of key features or vulnerabilities in the security system. These targets should become the focal points of the physical security system design.

As potential escape routes and tactical assets are identified, decisions must be made about the extent of vulnerability to escape that they represent. The natural focus of security system design is to harden those features or areas that are most obvious and likely to be used in an escape attempt. Each improvement moves the attention of

the potential adversary to the next easier path of opportunity. The cost of each proposed improvement can be measured against the reduction in vulnerability to determine its worthiness for consideration. As the level of vulnerability decreases, we eventually reach the point of "acceptable risk" below which we are willing to accept the vulnerability because additional security is not worth the cost.

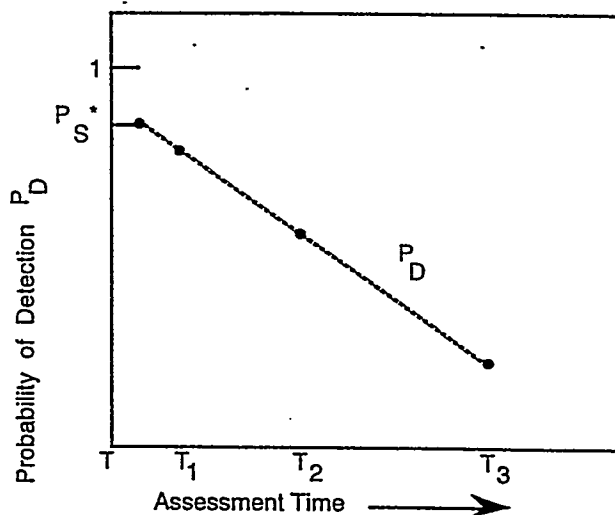
There are several functions that the physical security system must perform. It is essential to consider the system functions in detail, since a thorough understanding of the definitions of these functions and the measure of effectiveness of each is required to evaluate the system. The primary PSS functions are detection, delay and response.

Detection is the discovery of an adversary action. It includes sensing of covert or overt actions and requires that the following things must happen:

- A sensor, which could be a device or person, reacts to an abnormal occurrence and initiates an alarm.
- The information from the sensor and assessment subsystems is reported and displayed.
- A person assesses information and judges the alarm to be valid or invalid.
 - If assessed to be a nuisance alarm, a detection has not occurred.
 - Detection without assessment is not considered detection.

The measures of effectiveness for the detection function are the probability of sensing adversary action and the time required for reporting and assessing the alarm. Probability and time may be related as shown in Figure 1. A sensor activates at time T . Then at a later time such as T_1 , T_2 , or T_3 , a person receives information from the sensor and assessment subsystems. If the time delay between when the sensor activates and when the alarm is assessed is short (T_1) the probability of detection, P_D , will be close to the probability that the sensor will sense the unauthorized action, P_S . The probability of detection decreases as the time before assessment increases.

*Figure 1.
Probability of
Detection vs. Time
Between Sensing
and Assessment*



* Probability that sensor alarms

Detection can also be accomplished by corrections officers or other personnel. COs at fixed posts or on patrol may serve a vital role in sensing a prohibited action. Other staff personnel may contribute to detection by being vigilant during performance of their normal duties.

An effective assessment system provides two types of information associated with detection:

- Information about whether the alarm is a valid alarm or a nuisance alarm.
- Details about the cause of the alarm—what, who, where, and how many.

Delay is the slowing down of adversary progress. Delay can be accomplished by barriers, locks, and activated delays. The COs can be considered elements of delay if they are in fixed and well-protected positions from which they can execute use of force consistent with local statutory and facility policy. The measure of delay effectiveness is the time required by the adversary (after detection) to bypass each delay element. Any delay encountered by the adversary prior to detection is of no value to the effectiveness of the physical security system since a security force cannot respond to an escape attempt that it does not know is occurring. Furthermore, it does not provide additional time to respond to the adversary. Barriers and other forms of delay that are placed before the first alarm point only serve to direct adversary actions away from certain sequences or paths.

The response function typically consists of the actions taken by COs to prevent adversary success, usually the successful interruption of an escape attempt. The measure of response effectiveness is the time between receipt of a communication of adversary action and the neutralization of the adversary action.

The PSS must perform the functions of detection, delay, and response. These functions must be performed in a period of time that is less than the time required for the adversary to complete his tasks.

Figure 2 shows the relationships between adversary task time and the time required for the physical security system to do its job. The total time required for the adversary to accomplish his goal has been labeled Adversary Task Time. It is dependent upon the delay provided by the physical security system.

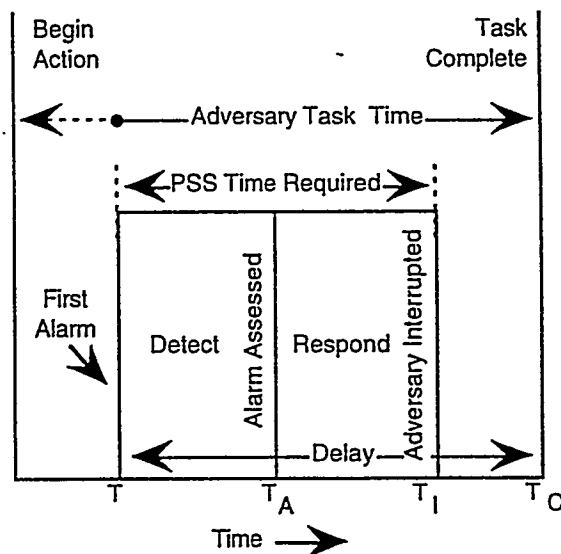


Figure 2.
Adversary Task
Time to PSS Time
vs. Requirements

The adversary may begin his task at some time before the first alarm occurs, labeled T in Figure 2. The adversary task time is shown by a dotted line before this point because credit cannot be taken for delay before detection - the clock starts when the alarm comes in. After alarm annunciation, the alarm information must be reported and assessed to determine if the alarm is valid. The time at which the alarm is assessed to be valid is labeled T_A , and at this time the location of the alarm must be communicated to the members of the response force. Further time is then required for the response force to respond in adequate numbers and with adequate equipment to interrupt and neutralize the adversary actions.

The time at which the response force interrupts adversary actions is labeled T_I , and adversary task completion time is labeled T_C . Clearly, in order for the physical security system to accomplish its objective, T_I must occur before T_C . It is equally clear that detection (the first alarm) should occur as early as possible and T (as well as T_A and T_I) should be as far to the left on the time axis as possible.

The perimeter of a corrections facility forms the interface between the controlled institutional environment and the outside world that expects to be protected from the convicted criminals confined by a lawful jurisdiction. The primary (but not the only) design objective of the perimeter security system is to prevent inmates from crossing this boundary undetected into the outside world and to allow time for the response force to apprehend the fleeing

inmates.

5. Outcomes

The perimeter security system is a collection of components or elements that, when assembled in a carefully formulated plan, achieve the objective of confinement to a high degree of confidence. Keeping in mind that confinement is the ultimate objective, it is clear that anyone attempting to escape the institution by crossing the perimeter must be interdicted by responding officers before the perimeter is successfully penetrated. The perimeter system must ensure that this confrontation can occur.

5.1 Fenced Perimeter

Figure 3 (not drawn to scale) shows a cross section cut through a basic two-fence security perimeter. It illustrates the components of a perimeter system and their relationship to each other. The perimeter itself is delineated by two chain-link fences with an isolation zone between them. All of the other components shown, including the camera towers and lighting, make up the security system applied to the perimeter which must incorporate the functions of detection, assessment, and delay, all facilitating an armed response to the point at which an escape is being attempted.

Fenced Perimeter

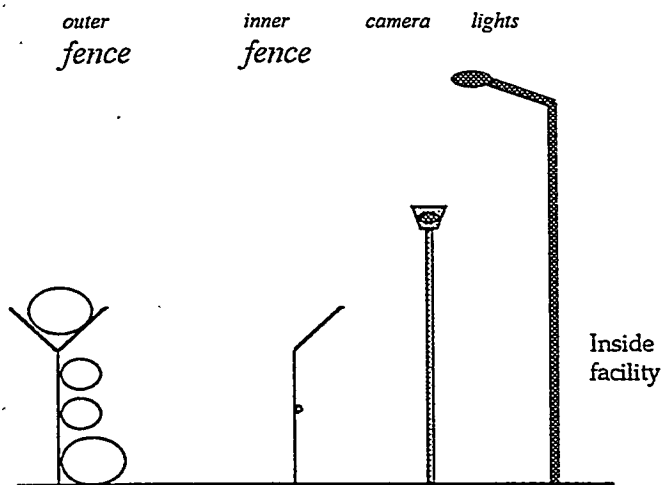


Figure 3. Typical Fenced Perimeter

The detection function is depicted as a fence disturbance sensor, such as an FPS-2, E-Flex, Guard Wire, Inertia Guard, Intrepid, or Intelliflex, attached to the *inner* fence. The sensor is placed to detect either cutting or climbing of the inner fence. An alarm from this sensor must be communicated back to a central reporting point at which the event is enunciated and its location reported to the corrections officer on monitor duty. A fence disturbance sensor was chosen as the primary means of detection for this type of perimeter due to nuisance alarm and vulnerability considerations, in coordination with the use of a CCTV assessment system.

Assessment and validation of the alarm condition is the next essential step. In the figure, this is accomplished by video assessment cameras placed inside the inner fence, positioned to assess alarms generated by sources approaching the fence from that side. They are set back from the fence to view the sensor zone obliquely and far enough back from the start of the sensor zone so that the entire zone can be viewed on screen.

The lens focal length should be chosen and the camera aimed so that the assessment zone of interest fills that major portion of the video monitor screen. This will provide the best resolution possible for assessment of the source of the alarm. The depth of field of the lens must be considered in focusing on the assessment scene. Under the lighting

conditions that fully open the lens aperture, the camera should be focused so that as much as possible of the sensor zone is in focus, particularly at the farther end of the zone. At the farther end of the zone, objects of interest in the assessment process will be their smallest, and so must be in better focus for validation purposes than at the near end of the zone where the objects are much larger. The design objective of the video assessment system is to be able to discriminate between person-sized alarm sources that could be escaping inmates and small animals or other sources of nuisance alarms.

Since video alarm assessment must be done at all times of the day or night, adequate lighting of the sensor zone is required at night. Adequacy is determined both by minimum available light level and light-to-dark ratio over the whole scene. For most practical purposes, the *minimum* light level at the sensor should be about 1 foot-candle and the light-to-dark ratio should not exceed 6 to 1 (the brightest portions of the scene should read no more than 6 times brighter than the darkest portions); while a ratio of less than 4 to 1 is strongly suggested for exterior lighting. This includes the entire area observed by the camera and not just the area of interest. That is, lighting must extend beyond corners and fences to provide even illumination over three-fourths of the camera field of view. The area of primary interest should be uniformly light-colored with a minimum reflectance of 30% when dry. Lighting fixtures should be chosen to deliver adequate light levels when placed at sufficient height to give reasonably even distribution. The spacing of the light standards will then be determined by the light-to-dark ratio. Light standards must be set back from the inner fence far enough to assure that the inner fence is evenly illuminated from top to bottom.

The camera towers should be high enough to place the cameras such that they look down on the assessment scene so that the lighted horizon never appears in the field of view, but below the light fixtures so that the light fixtures are never included in the assessment scene.

The outer fence in the figure is shown with a barrier delay system installed on it. In this case, a series of razor-ribbon coils are firmly attached to the inner vertical surface and on the top of the fence. The coils on the fabric portion of the fence are placed to prevent access to the fence for purposes of either cutting or climbing. The lower coil is sized, placed, and attached to prevent access to the bottom of the fence for tunneling under it or prying it up from the ground. The spacing of the coils is such that it limits access to the fence fabric and precludes climbing between them. The coil on the top of the outer fence is positioned to impede climbing over the fence. The barrier system must provide enough delay so that the response force will have time to move into position to intercept the escapee before he can penetrate or clear the fence.

The isolation zone between the inner and outer fence must be wide enough to prevent bridging of the sensor and barrier system by any practical means. It must also be wide enough to permit convenient cleaning and maintenance of the zone. The isolation zone serves the purpose of preventing undetected access to the outer barrier system. It also forms a linear confinement zone in which the escapee is trapped after triggering an alarm and while the response force is en route. This limits the area that the response force must cover when they get into position.

The perimeter system presented above represents the basic perimeter security system that meets the operational security requirements of Maximum, Close, and Medium Security Level facilities.

At Minnesota Correctional Facility-Lino Lakes, a modified version of these standards was adopted. It is significant that there is a residential neighborhood within three hundred yards of the facility. Even though the prison predates the housing development, the development predates renovation of the perimeter and the effect of security upgrades on the neighborhood had to be considered.

The existing lighting was inadequate for the addition of cameras. Any increase in visible lighting would disrupt the neighborhood. Visible lighting which activated upon receipt of alarms would potentially panic the neighbors. Therefore, infrared spotlights which activate upon receipt of alarms were placed on standards between the perimeter fences. Existing visible lighting was upgraded to low pressure sodium. Thus, all standards for lighting and neighborhood considerations were met.

To save the cost of duplicate standards, cameras capable of detecting light across infrared and visible light spectrums were mounted on the same poles next to the infrared spotlights.

Corroded fence fabric was replaced and several coils of razor ribbon were distributed between the fences.

5.2 Walled Perimeter

A perimeter security system that includes a high stone or concrete wall would be more typical of a security upgrade of an existing prison with a perimeter wall than of new construction. There are two basic design approaches applicable to this situation. In one approach, the wall could be viewed as analogous to the outer fence of the system shown in Figure 3. Sensors, video cameras and lighting could then be added to the configuration in much the same way as discussed above for the fenced perimeter.

A second approach would be to take advantage of the height of the wall, typically about twenty feet, and install sensors and additional delay barrier on the wall. In an existing facility with a long operating history, it is very likely that the entire yard enclosed within the wall is being utilized for inmate activity. It is understandable that there would be reluctance to relinquish the use of yard space to allow establishment of an isolation zone inside the wall. For these reasons, and to take full advantage of existing walls, the second approach will be discussed here.

The generally accepted means of defeating a high wall is the use of a ladder or a grappling hook and rope. The same defeat mechanisms apply to buildings that form a part of the perimeter. A physical security system installed on a wall or building must therefore counter this threat. The system shown in Figure 4 is based on a twenty-foot high wall with a thickness at the top of sixteen to twenty four inches. The construction is assumed to be solid stone masonry or reinforced concrete which should discourage attempts to cut through the wall. Lighting standards are also shown mounted on the top of the wall since this was typically done in the walled facilities.

Walled Perimeter

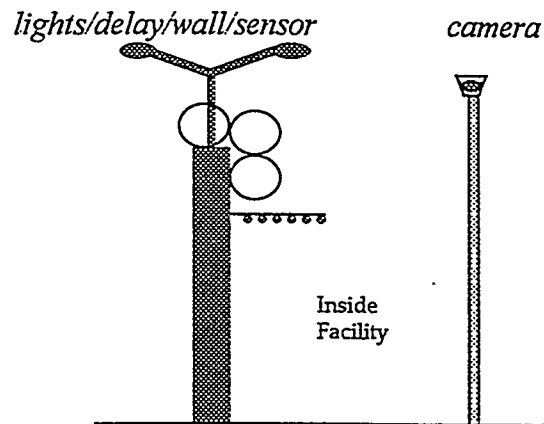


Figure 4. Typical Walled Perimeter

The detection system shown in Figure 4 is a multiple-wire capacitive array type of sensor which is typically used either free-standing or mounted to a chain link fence. In this application, the array would be mounted on the wall about fifteen feet above the ground. The array should extend inward five or six feet from the wall, but at least as far as the arm of the light standard extends. The sensor is placed to detect a climber approaching the top of the wall, and extends inward far enough to detect a ladder or other climbing aid being leaned against the wall or a grappling hook and rope thrown over the wall or the light standard, all of these threats coming from the inside. The same sensor would detect adversaries scaling the wall from the outside since there would be no convenient way to get over the wall and inside the yard without encountering the sensor array. The type of sensor array suggested in this figure is made up of very thin wires spaced several inches apart. It is not nearly as sensitive to birds landing on these wires as one might expect because the birds are not electrically grounded. The wires must be displaced significantly to vary the electrical capacitance of the array enough to trigger an alarm.

The assessment system shown is composed of fixed focal length video cameras located inside the wall and positioned essentially as those used for the fenced perimeter. In this case, however, the zone of essential assessment interest may be considered as limited to the sensed area near the top of the wall. However, as in the discussion above for the fenced perimeter, the camera towers must be tall enough to prevent the cameras from seeing above the horizon, and they must be aimed to keep the lighting fixtures out of the assessment scene. In most cases, these conditions will result in most of the wall and some of the ground leading up to the wall being covered by the field of view. This will allow observation of the source of ropes or climbing aids that may have triggered the alarm.

Adequate lighting of the assessment scene in this configuration presents more of a design challenge than the fenced perimeter. If the lighting fixtures are located on top of the wall, they will be from ten to fifteen feet from the sensor array in the vertical direction, and five or six feet inboard of the wall. This will produce hot spots in the lighted field of view that will exceed acceptable light-to-dark ratios. A solution to this problem would be to add more light sources along the wall, and reduce their intensity or direct them away from the surface of the wall.

The barrier delay system shown consists of three coils of razor tape deployed above the sensor, along the inner face of the wall and along its top. There is essentially no distance between the sensor and the top of the wall. A determined adversary may therefore be willing to concede detection based on his ability to clear the wall before the response force can arrive. The razor tape barrier is placed to preclude any access to the top of the wall and thus to prevent climbing over the top. The lighting standards could be used to bypass the barrier. They should therefore be designed or modified to break away when heavily loaded.

In this vertically oriented configuration, there is no isolation zone in the sense discussed for the fenced perimeter. The vertical face of the wall serves many of the same tactical purposes as the isolation zone. The advantage of the vertical arrangement, with the sensors and barriers at the top of the wall, is that any attack on the system must be carried out at a deterring height above the ground. There is no way of casually engaging either the sensor or the barrier.

The walled perimeter system presented above represents the basic perimeter security system that meets the operational security requirements of older Maximum, Close, and Medium Security Level facilities.

The work of Sandia National Laboratories and cost estimates obtained by staff at Minnesota Correctional Facility-Stillwater fulfill the requirements of the predesign study requirement. However, the facility has not been successful in the political arena, because this project was weak competition in comparison to nearly one hundred million dollars of higher prioritized corrections projects, including a \$89 million, 800 man close security prison.

6. Lessons

The most important lesson learned can be summarized in the word "partnerships." During negotiations with the architects and security consultants, Minnesota Department of Corrections was able to use the unique capabilities of Sandia National Laboratories to better determine their own needs, prevent mistakes, arrive at solutions to problems, and help to refine construction plans. At the same time, Sandia was able to leverage security-related lessons learned back into their role as the Department of Energy's Lead Laboratory in Physical Security, which involves knowledge and experience in high security systems engineering, as well as associated research and development, test and evaluation, modeling and simulation, training, and standards activities. Hopefully, future partnerships involving Minnesota Department of Corrections, Sandia National Laboratories, architects, security consultant firms, and others such as the National Institute of Justice, the American Corrections Association, and other corrections agencies can further the development of such teamwork and provide more cost effective security at correctional facilities nationwide.

In addition, as design of the new 800 bed facility progresses in Minnesota, we hope to set up test grounds on the prison site which will yield scientific data upon which to base system decisions.