Nuclear Plant Security Systems

Gary W Castleberry, PE

Course Description

This course will introduce the student into the design of security systems for commercial nuclear power plants. An overview of plant security systems is provided along with a linkage to the Federal Requirements that govern commercial nuclear plant security systems. The course provides an understanding of the types of security systems utilized and their application.

IMPORTANT DISCLAIMER: The information in this course is not of a "classified" nature. The material presented is generic to the industry and no specifics about any individual plant security systems are provided.

Learning Objectives

Upon successful completion of this course, the student should obtain the following performance objectives:

- Defense in depth;
- Overview of nuclear plant security;
- Knowledge of the Federal Requirements;
- Understand the types of security equipment; and
- Basic understanding of the application of equipment.

Introduction

Commercial nuclear power plants, owned and operated by public utility companies, have been operating since the 1960's. The Federal Government issued licenses to the utility to build and operate the plants. The underlying theme in the design and operation of these plants has always been the protection of the health and safety of the public.

This was accomplished in the design through a design philosophy called defense in depth. Redundancy of safety components and systems were part of this defense in

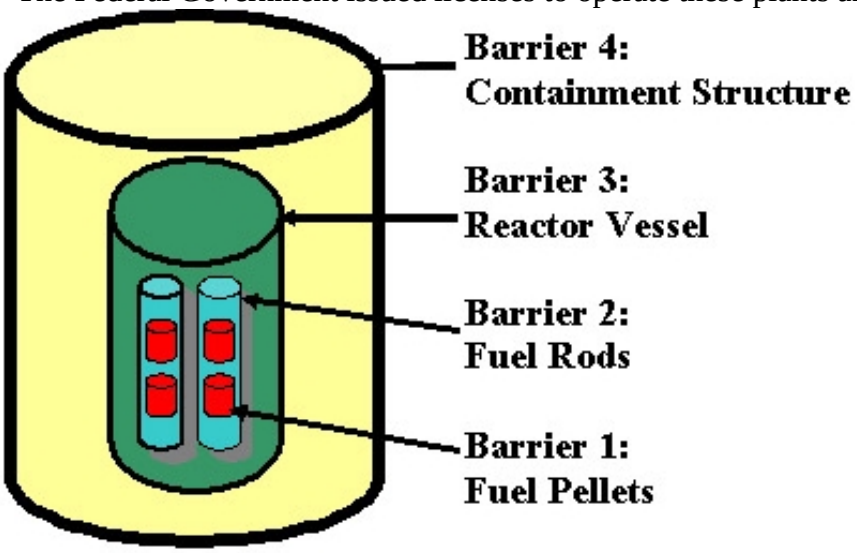
depth; also, robust structures that house the reactor contain any radiation in the event of an accident.

To protect the health and safety of the public from radiological sabotage at one of these facilities, strict regulations were established for the security programs. As a result of these original regulations and continuing changes to the regulations, commercial nuclear power plants are some of the best protected facilities in the United States.

Course Content

Part 1 Defense in depth

The nuclear power plants in the United States were built and operated by public utility companies. The Federal Government issued licenses to operate these plants after an



Defense in Depth via Four Barriers

extensive review of volumes of safety analysis reports. During the early days of nuclear power this governance was performed by the Atomic Energy Commission and in the early 1970s the Nuclear Regulatory Commission was formed to oversee commercial nuclear power.

The principle of design for nuclear power plants was defense in depth. Layers and layers of defense were put in place to assure the safety of the public. Some of the elements of the defense in depth philosophy are:

- **Redundant Safety Systems –** The systems necessary to support the safe shutdown of the nuclear reactor were designed with redundant and diverse

backup systems. Only the highest quality materials went into the building of these systems.

- **Automatic Reactor Protection Systems** – These systems monitored critical parameters of the reactor system and automatically initiate shutdown of the reactor when the parameter limits are exceeded.

- **Radiation Containment Barriers** – Four physical barriers are designed to prevent radiation from escaping and reaching the public.

    - Fuel Design – the nuclear fuel is composed of ceramic pellets which contain most of the radioactive material within the fuel pellet.
    - Fuel Rods – the nuclear fuel pellets are placed in metal tubes that are welded shut to prevent the release of any material.
    - Reactor piping system – the reactor and the piping associated with the reactor system is composed of very thick steel alloys and is a sealed system.
    - Containment Building – the reactor is housed in a steel and concrete building several feet thick. These building can withstand the force of hurricanes and the impact of airplanes.

- **Plant Security Systems -** Plant security systems in combination with highly trained guards and response teams protect the plant from acts of radiological sabotage.

There are several more aspects to defense in depth including the training programs, the selection of highly qualified personnel, and federal inspectors assigned to each plant on a full time basis. The four elements above have been presented in more detail due to the interaction the plant security program has with the first three elements.

Part 2 Overview of nuclear plant security

Security at a nuclear power plant is a very serious business. The security personnel are well trained professionals often with college degrees, backgrounds in law enforcement and/or the military. These armed security officers use a variety of high technology and sophisticated surveillance equipment to continuously monitor the areas around the nuclear facility. Drills are conducted on a frequent basis that simulates the attack of intruders armed with explosives and automatic weapons.

The security program is composed of the plant physical security systems, the security personnel, and several different written programs which define aspects of the security program.

The function of any security system is to accomplish three things: **detection, delay, and defense**. The first two functions combine to give the security force time to perform the third function: defense. To better understand this concept a look at the physical layout of the plant site is necessary.

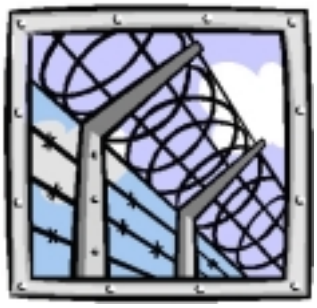
The physical land area of a commercial nuclear plant is divided into a number of distinct areas for security purposes. The analogy of a marksmanship target is often used to describe these areas. The innermost area akin to the bulls-eye on a target is called the Vital Area. The next outer ring is known as the Protected Area. The next outer ring of the target is known as the Owner Controlled Area.

VITAL AREA

The Vital Area contains structures, systems and components which are essential for the safe shutdown of the nuclear reactor. These components are often referred to as Safety Related Equipment with the connotation being “Nuclear” Safety not Industrial Safety. Examples of vital equipment include station battery banks and emergency high pressure injection pumps.

Access to vital areas is on a “need to be there” basis. Access to these rooms is controlled by locked doors which are monitored by access control computers. Only plant personnel whose job functions require them to access Vital Areas are approved for entry. Entry is accomplished by swiping your security badge through a reader, the access control computer verifies you are authorized entry and electronically unlocks the doors. If the vital area door is not closed within a few seconds, an alarm will be generated.

PROTECTED AREA



The plant proper is surrounded by a double fence with access controlled by the plant security department. All of the area within the double fence is known at the Protected Area. All personnel (and vehicles) that enter the Protected Area are searched and must have an approved access badge to enter or must be escorted at all times by an individual with a badge.

Within the Protected Area are four other important security locations. These are the:

- Isolation zone – this is the two twenty foot areas, one between the double fences surrounding the protected area and the first twenty feet within the second or innermost fence. The second isolation zone which is next to the inside fence on the protected area is usually marked by painted lines on the ground. These areas are kept clear of people, material and obstructions to allow unlimited observation by the security cameras and officers.
- Access Control Point - This is the gatehouse to the Protected Area and this is where egress and ingress to the Protected Area is controlled. Employees are searched, screened, and all packages checked prior to the employee entering the plant.
- Central Alarm Station (CAS) – a room which houses the monitors for the security equipment, terminals to the access control computer, and emergency communication equipment..
- Secondary Alarm Station (SAS) – This is a redundant facility duplicating the functions of the Central Alarm Station.

OWNER CONTROLLED AREA

All of the area outside the Protected Area, usually to the company's property border is referred to as the Owner Controlled Area. Access to the owner controlled area is generally restricted to personnel who have a business need to enter. During heightened states of national security, access to the owner controlled area can become restricted to critical company personnel only. The owner controlled area is patrolled and monitored by roving patrols.

One can now see how the actual physical design of the nuclear plant and the arrangement of the security zones help establish the detection function, the delaying function, and aid in the defense function.

Part 3 Knowledge of the Federal Requirements

The requirements for nuclear plant security systems are set forth in Title 10 of the Code of Federal Regulations Part 73 with the basic requirements in section 73.55. For more information on this subject visit the Nuclear Regulatory Commission website at www.NRC.gov and visit the electronic reading room. 10CRF73.55 also provides the requirements for the security organization, the various plans and documentation requirements; however, this course is focused on the security hardware and thus will summarize some of those key requirements. Part 73.55 specifies among others things that:

- All hand-carried packages are searched for radiological sabotage devices such as firearms and explosives.

- A vehicle barrier system surrounding the protected area to prevent a vehicle bomb attack.
- Lighting around the protected area to a minimum level of .2 foot-candles measured horizontally at ground level.
- Bullet resistant doors, ceilings and walls for the plant control room.
- Identify and search all persons entering the protected area.
- Inspect all packages delivered to the protected area for sabotage devices.
- Inspect all vehicles entering the protected area for sabotage devices.
- A numbered badge system for employees.
- Positively control all points of entry to the vital areas.
- Bullet resistant central alarm station to which all alarms annunciate.
- Bullet resistant secondary alarm station to which all alarms annunciate.
- All alarming devices must be tamper indicating.
- Communication equipment between the officers and alarm stations.
- Communication equipment between the alarm stations and outside authorities.
- Detection of attempted or actual entry to the protected area by unauthorized personnel. This requirement determines the need for much of the perimeter intrusion system installed at nuclear plants.

These requirements are based upon what is deemed necessary to deal with what is called the design basis threat. The design basis threat is a given scenario that in turn established the basis for the design of the security systems. The Federal Government provides that design basis threat information in 10CFR Part 73.1. In summary, the

threat is an attack by a determined and well trained of several individuals equipped with automatic weapons and explosives. They may be helped by a knowledgeable person inside the plant who may either aid in a passive role (provides information) or active role (disrupts alarms and communications). The second design basis threat is an attack by a four wheel drive vehicle carrying a bomb. The third design basis threat is the work of any employee who conducts acts of nuclear sabotage. Understanding the design basis threats is necessary in order for the design engineer to understand the types of security equipment required to mitigate these threats.

Part 4 Understand the types of security equipment

Most of the plant security equipment is found in the following three physical areas of the nuclear plant.

- The isolation zones. Here the perimeter intrusion alarm systems are located.
    - Microwave intrusion detectors – Highly sophisticated transmitters and receivers used to detect the motion of people between the outer and inner protected area fences.
    - Vibration monitors – Devices which detect vibration due to tampering or attempting to climb the monitored surface such as a fence or wall.
    - E-fields - Another form of intrusion detection system that uses electric fields to monitor the proximity of intruders.
    - IR Fields - Light beam intrusion alarm systems which work in the infra-red light spectrum
    - Closed circuit televisions (CCTV) – a system of cameras on a dedicated network used to monitor the isolation zones.
    - Perimeter fences – the barriers surrounding the protected area.
    - Delay devices – devices intended to delay intruders until response teams are in place
- The Central Alarm Station and Secondary Alarm Station
    - Control panel – custom consoles that house the CCTV monitors and usually terminals for the Access Control Computer
    - CCTV monitors – a bank of several monitors that provide a complete picture of the protected area

- CCTV switch – an electronic switch that can produce a programmed sequence of camera view.

- Access Control Computer – Process control computers that control access to the vital areas.

- Communication Equipment – radios, hard-wired land line telephones, and cellar phone communication systems used to maintain contact between all of the security officers and the CAS/SAS and between the CAS/SAS and the outside authorities.

- The access control point.

  - Metal Detectors – walk through portal devices which alarm on any metal objects on the individual

  - Explosive Detectors – walk through portal devices that sense the presence of chemical residue that could be explosive material.

  - X-ray Machines – machines for x-ray parcels being brought into the plant.

  - Key card readers – Electronic swipe stations that read magnetic stripe employee badges in order to open a locked door

  - Biometric door controls – devices that measure parameters of the human body to identify an individual against a pre-recorded set of measurement.

  - Turnstile Cages – single direction only, rotating cages which control access into and out of the plant.

Part 5 Basic understanding of the application of equipment

- The isolation zones. Here the perimeter intrusion alarm systems are located.

- Microwave intrusion detectors – Highly sophisticated transmitters and receivers used to detect the motion of people between the outer and inner protected area fences. A microwave system is made of a series of overlapping links where each link is a transmitter and receiver separated by distances of 500 to 700 feet. Each link feeds into a multiplexer that monitors each link for intrusion alarms, tamper alarms, and low voltage alarms. These units operate on the microwave X band (10GHz) and newer units on the K (24 GHz) band. Placement and tuning of these links requires a certain amount of expertise to assure there are no "holes" an intruder could use. The electronics on these devices must be tuned for different type of intrusion as a runner, slow walker, or "belly-crawler" all have different "signatures" to the equipment. Once installed and properly calibrated, microwave intrusion systems are nearly impossible to defeat.

- Vibration monitors – Devices which detect vibration due to tampering or attempting to climb the monitored surface such as a fence or wall.

- IR Fields - Light beam intrusion alarm systems which work in the infra-red light spectrum. IR detectors are useful for providing a short link in a perimeter intrusion alarm system where microwave detectors may be impractical. Vertical poles housing multiple transmitters and receivers from an invisible series of beams that alarm when penetrated.

- Closed circuit televisions (CCTV) – a system of cameras on a dedicated network used to monitor the isolation zones. Placement of the cameras is the critical task a security engineer performs. These cameras may be fixed or of the pan, tilt, and zoom type. Regardless of type, the engineer must assure that the

isolation zones have 100% coverage and that coverage is maintained at all times. Placement of the cameras must account for the rising and setting of the sun, in all seasons, to prevent blinding of the camera.

- Perimeter fences – the barriers surrounding the Protected Area. The fences form part of the delay barrier into the Protected Area. The inner fence is the real barrier as required by the code of federal regulations. This is the barrier that is being monitored by the intrusion equipment to detect the intruder. The outer fence is really a barrier to prevent accidental alarms by innocent individuals; however, it does serve an additional function of delaying intruders such that the CCTV does have an early opportunity to identify the intrusion.

- Delay devices – devices intended to delay intruders until response teams are in place. A delay device may be additional fencing with gates with simple latches that delay an intruder sufficiently for the response team to deploy.

- The Central Alarm Station and Secondary Alarm Station

  - Control panel – custom consoles that house the CCTV monitors and usually terminals for the Access Control Computer. These panels are custom designed for each station and allow one or two operators to access all controls, alarm responses, and camera monitors. Communications equipment is usually installed with the console along with terminals to access the access control computer.

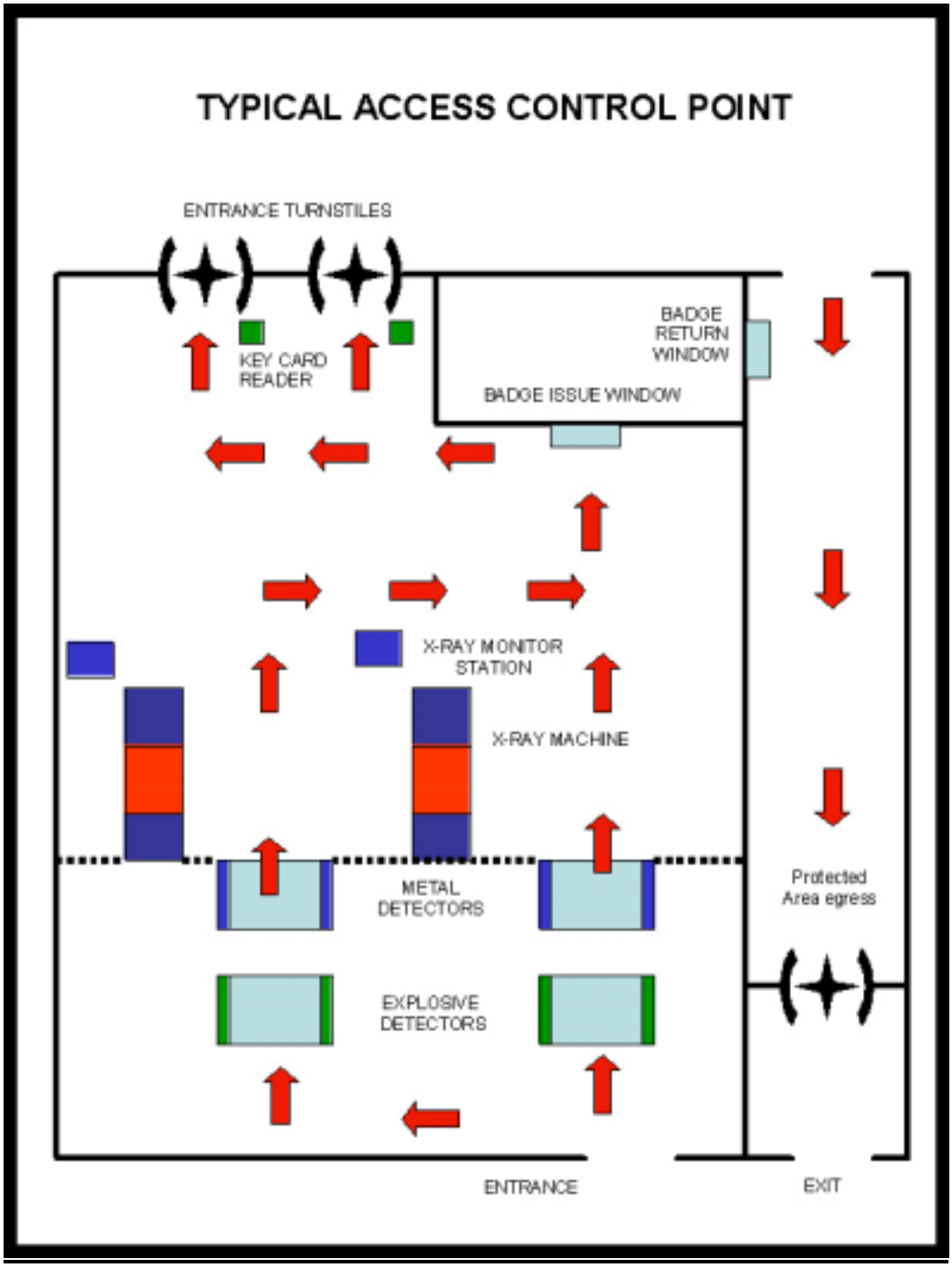
  - CCTV monitors – a bank of several monitors that provide a complete picture of the protected area

  - CCTV switch – an electronic switch that can produce a programmed sequence of camera view.

  - Access Control Computer – Process control computers that control access to the vital areas.

  - Communication Equipment – radios, hard-wired land line telephones, and cellar phone communication systems used to maintain contact between all of the security officers and the CAS/SAS and between the CAS/SAS and the outside authorities.

- The access control point. A simplified sketch of an access control point is presented here to help the student understand the traffic flow and arrangement of the equipment.



- Explosive Detectors – walk through portal devices that sense the presence of chemical residue that could be explosive material. The individual must walk into the detector enclosure and pause for several seconds while air samples are drawn into the machine and analyzed. Modern explosive detectors will detect several types of explosives. There is no required order for whether people must pass through the

metal detector first or the explosive detector first. The sketch of a typical access control point in this course shows the explosive detectors first. The metal detectors need to be close to the x-ray machines for convenience of removing objects from your pockets and placing them in the x-ray machine before passing through the metal detector.

X-ray Machines – machines for x-ray parcels being brought into the plant. These machines are familiar to anyone who has traveled by commercial airlines. Briefcases, packages, lunchboxes etc. are placed on a moving conveyor belt and passed through an x-ray device. The operator has a monitor to view the contents. Modern high tech x-ray machines have color monitors that will highlight contraband material such as narcotics or explosives with a preprogrammed distinct color. The design engineer should check with the vendor of both the x-ray equipment and the walk through metal detector for any issues regarding electro-magnetic interference between the two devices. Older metal detectors are prone to this problem.

- Metal Detectors – walk through portal devices which alarm on any metal objects on the individual. Again, a familiar device for anyone who flies on commercial airlines. The metal detectors today have become quite sophisticated from the ones first placed in use in airports thirty years ago. Today's models can provide the security screener with the location on the body and an estimate of the size of material. The detectors will detect metal objects hidden in body cavities.

- Key card readers – Electronic swipe stations that read magnetic stripe employee badges in order to open a locked door. Similar to the card swipe machines located at nearly every cash register today, these card readers send the scanned data back to the access control computer. The access control computer validates the card as legitimate and that the person is authorized access for that door. Card readers are used for station accountability drills during emergencies allowing for the rapid determination that all station personnel are accounted for and located.

- Biometric door controls – devices that measure parameters of the human body to identify an individual against a pre-recorded set of measurement. Biometrics is a rapidly growing science that has been around for about twenty years. Biometric devices when coupled with a key card make positive identification of an individual prior to entry to the protected area. The most widely used system at nuclear plants today is called hand geometry. A hand geometry reader is a device in which your hand is placed on a flat surface with several pegs. Your must place your hands in an exact configuration governed by the peg locations. A camera scans your hand and makes several dimensional measurements.

This is compared against a pre-recorded baseline and if a sufficient number of measurements agree access is granted.

- Turnstile Cages – single direction only, rotating cages which control access into and out of the plant. These devices are floor to ceiling rotating doors similar to building rotating doors except they use metal bars instead of glass. Turnstile cages will only accommodate a single individual and only move in one direction. They are unlatched by a solenoid latch activated by the access control computer.

Glossary

- Biometric – the electronic measurement of human body attributes to establish identity
- CFR – Code of Federal Regulations
- CAS – Central Alarm Station – a room which houses the monitors for the security equipment, terminals to the access control computer, and emergency communication equipment..
- Contamination – the presence of radioactive material where it is not desired.
- Delay devices – devices intended to delay intruders until response teams are in place.
- Isolation zone – this is the two twenty foot areas, one between the double fences surrounding the protected area and the first twenty feet within the second or innermost fence.
- Microwave intrusion detectors – Highly sophisticated transmitters and receivers used to detect the motion of people between the outer and inner protected area fences.
- Owner Controlled Area – the plant property outside the double fences surrounding the plant
- Program – a set of procedures which implement a required set of tasks such as welding
- Program Owner – the department responsible for administrating a program
- Protected Area – the area within the double fences which surround the power plant
- NRC – the Nuclear Regulatory Commission
- Radiation – the energy that is emitted from an unstable atom
- RCA – Radiation Controlled Area
- Radioactive Material – substance, matter, material that emits radiation due to this natural decay process
- SAS – Secondary Alarm Station – the redundant security control room.
- Vital Area – areas of the plant containing equipment necessary for the safe shutdown of the reactor

Conclusion

This course has introduced the student to the design of security systems for commercial nuclear power plants. An overview of plant security systems has been provided along with a linkage to the Federal Requirements that govern commercial nuclear plant security systems. The course has provided an understanding of the types of security systems utilized and their application. The knowledge gained from this course is applicable to the design of good security systems for any valuable asset.

As the threats to the nation and to our vital assets, nuclear power station, the regulations and designs of the security systems will change to meet that threat.

IMPORTANT DISCLAIMER: The information in this course is not of a "classified" nature. The material presented is generic to the industry and no specifics about any individual plant security systems are provided.