# A Security Approach for the Example Sodium Fast Reactor

Christian Young, Dr. Robert Bean

*Purdue School of Nuclear Engineering, West Lafayette, Indiana, United States of America*

## Abstract

Increases in the spread of nuclear technology and the rise of non-state terrorism in the modern era has proved the need for effective security approaches to new nuclear facilities. Many documents about security approaches for nuclear plants are non-public material, however, making it difficult to teach others about the basics of security design. To alleviate this issue, we used available texts in the security realm to design a security approach for the Generation IV International Forum's Example Sodium Fast Reactor. Our approach utilized infrared, microwave, fiberoptic, and other advanced technologies to provide security for the special nuclear material present. While this is not meant to be a final approach for any one facility, it serves as an example for those wanting to learn about how to design security systems for both nuclear and non-nuclear plants.

## Introduction

With the rise in terrorist activities in the 21st century, national security has been a key focus in the international community. Attacks on facilities and instances of theft of fissile material have shown to us that nuclear terrorism is a real threat [3]. Many international organizations, including the United Nations and the International Atomic Energy Agency, have put out documents and treaties discussing the importance of nuclear security [7,8,9]. Along with these, a recent paper by Charles Bathke outlines the desirability of many nuclear materials present at power plants for use in nuclear weapons [2]. The higher enriched materials discussed in Bathke's paper are especially common at more modern reactor facilities, like fast reactors [2]. It is clear that securing nuclear facilities is becoming an important issue amongst both governmental bodies and scientists alike.

There are several documents available on how to secure nuclear power plants, though they all share similar flaws. Mary Lynn Garcia's book *The Design and Evaluation of Physical Protection Systems* offers advice on how to secure a nuclear facility. The book goes in-depth on various devices used for detecting adversaries and for controlling sites [4]. The book, however, does not go into detail about how a nuclear facility should specifically be laid out, and it does not provide any example facilities to utilize the book's suggestions [4]. Matthew Bunn's paper talks at length about how governing bodies can prevent nuclear terrorism, but the paper discusses very little about the actual security measures needed at a nuclear facility [3]. Generation IV International Forum's *Proliferation Resistance and Physical Protection* analysis does a great job looking at the fundamentals of physical protection [1]. This evaluation is also incredibly useful for its ability to connect people from the safeguards world to people in the security world [1]. In terms of actual physical protection planning, however, the report does not discuss methods for how to actually prevent terrorists from getting into the plant; it only approximates how long a terrorist might take to break into a facility and what, very generally speaking, would get in their way [1].

This paper is meant to address these issues by using the Generation IV International Forum's Example Sodium Fast Reactor (ESFR) as a base facility and designing a specific physical protection system for it. We cannot use any pre-existing nuclear power plant, like Point Beach Nuclear Generating Station, for example. Documentation of security systems for pre-existing

nuclear plants is non-public material. The ESFR, however, is a publicly available example system, so any analysis done with it can be public knowledge. Information about the protection of nuclear plants is valuable to the nuclear community. This paper will help serve as a guide for other groups trying to understand the complexities of nuclear physical protection systems' design and analysis. The Generation IV International Forum has already done a basic form of security analysis on this plant, which will help guide us through the process of physical protection system design [1].

To design a security system for this power plant, we will be using a couple of texts as guides. Mary Lynn Garcia's book *The Design and Evaluation of Physical Protection Systems* will provide us with the basics on how to secure a nuclear facility [4]. The book goes into great detail about each component in a physical protection system and their various pros and cons [4]. This book, however, is older, so we will implement newer technology not discussed in the book to strengthen our security plan. Included in this plan will be methods for determining the design basis threat of the system created by the IAEA [6]. This will help us understand what adversaries our plant may be facing.

To analyze our physical protection plan and locate any vulnerabilities during the design phase, we will be using methods from *Vulnerability Assessment of Physical Protection Systems* by Mary Lynn Garcia and the United States Army War College's *Strategic Wargaming Series Handbook* [5, 10].

## Design Methodology

The three main parts to a physical security approach are the design basis threat (DBT), the physical protection plan, and any analysis of the plan. There are many texts associated with each of these three key points. This section will discuss the texts used and why they are relevant.

### *Design Basis Threat*

The creation of the design basis threat is aided by the International Atomic Energy Agency's publication *Development, Use, and Maintenance of the Design Basis Threat.* According to this publication, there are three phases when creating your DBT, which are listed as "screening the threat assessment, translating data on specific threats into representative adversary attributes and characteristics, and modifying representative adversary attributes and characteristics on the basis of policy factors" [6]. We will be following this exact recommendation as we design our DBT.

### *Physical Protection Plan Design*

Mary Lynn Garcia's *The Design and Evaluation of Physical Protection Systems* will be the guiding text for creating the physical protection plan. This book provides details into several components used to detect and deter adversaries [4]. Placement of these devices and why they were chosen are largely based off of the recommendations of this book.

### *Physical Protection Plan Analysis*

The previously mentioned book, along with Garcia's *Vulnerability Assessment of Physical Protection Systems,* will help guide us through the analysis of our physical protection plan. Both books provide statistical data to analyze security components, and both offer links to publicly available tools used in the industry [4,5]. On top of this, we will be using a simplified tabletop exercise to find vulnerabilities in the security plans. For our wargame, we will borrow concepts

from the *Strategic Wargaming Handbook*, allowing us to better simulate an attack on the facility [10].

## Development

### *Design Basis Threat*

*Description*

For our facility, we are planning to defend against up to ten adversaries. This group of adversaries will be armed with a wide range of tools, such as cordless drills, saws, and grinders, torches, and ladders. The group will have access to vehicles; we predict that for ten adversaries we will have two vehicles.

Adversaries should be expected to be well armed. They will have access to several types of firearms, like pistols, rifles, and crew-serviced weapons. They will also have a variety of explosives available to them. Adversaries are expected to use vehicle-borne improvised explosive devices, shaped charges, and suicide bombs. Shoulder-mounted rockets or rocket propelled grenades are not considered in this design basis threat.

Adversaries should be assumed to have full knowledge of the plant's interiors and exteriors. They should also be expected to not surrender during the assault. The groups we are planning for are ideologically motivated and will stop at nothing to get their hands on special nuclear material.

*Context*

As mentioned previously in this paper, the goal of this physical protection approach is to stop well-armed non-state actors. Though a country's military force could be a potential adversary group, the wider reaching political and social climate surrounding an invasion would make analysis of a physical protection plan incredibly difficult. Should this happen, the host country's military would most likely take over protection of the plant.

A group of ten well-armed terrorists might seem like an extreme case to defend against. It is important to realize the consequences of a successful attack. Should a group steal material present at this facility, they would have the capability to build a nuclear weapon, as Charles Bathke's paper *The Attractiveness of Materials in Advanced Nuclear Fuel Cycles for Various Proliferation and Theft Scenarios* demonstrates that most material present would be "desirable" for theft [2]. Though the chance of an attack of this magnitude is low, the consequences are high, which makes this design basis threat valid.

### *Physical Protection Plan Design*

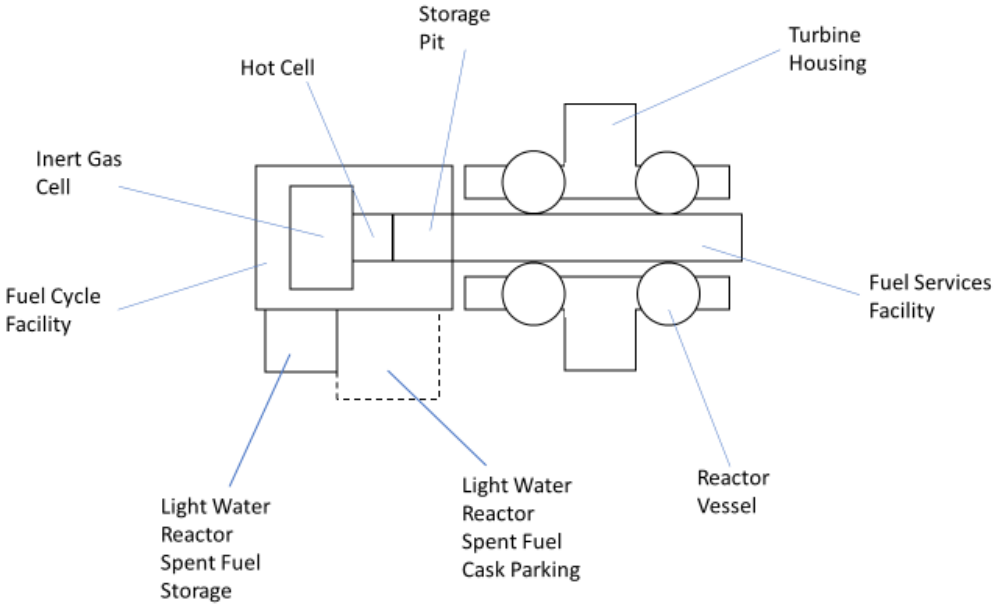


Figure 1. An overview of the ESFR layout

To understand the reasons behind the security approach, it is useful to know the basics to the operation of the ESFR provided by the Generation IV International Forum [1]. The ESFR, as the name suggests, uses liquid sodium metal to cool off then fuel present in the reactor. The fuel is of a higher enrichment than your standard light water reactor fuel. That is common in a fast neutron reactor. To minimize the vulnerabilities of transporting such highly enriched fuel, fuel fabrication and reprocessing is done on site. Shown in Figure 1, there are nine areas marked in our report. All but one of them, the turbine housing, will be discussed in the design of our security approach.

- Light Water Reactor Spent Fuel Cask Parking: This parking area holds shipping containers containing spent fuel from typical light water reactor power plants.
- Light Water Reactor Spent Fuel Storage: Once spent fuel has been unloaded from the casks, it goes here to be stored.
- Fuel Cycle Facility: The Inert Gas Cell, Hot Cell, and Storage Pit are enclosed in this area. Plant workers operate machines from this area.
- Inert Gas Cell: Fuel reprocessing is done here. Light Water Reactor fuel, along with spent fuel from the ESFR, are separated into their components. New fuel slugs are made here.
- Hot Cell: Disassembly and reassembly of ESFR fuel is done in this area.
- Storage Pit: ESFR fuel is stored here until it is ready to be disassemble or put back into a reactor.
- Fuel Services Facility: Used ESFR fuel assemblies are washed of their sodium and new ones are prepped to enter the reactor.
- Reactor Vessel: This is what holds the ESFR. Note that there are four reactors at our example plant.

- Turbine Housing: This area contains the water vapor turbines and all heat exchangers between the molten sodium and the water.

Our security approach to this facility starts with fence placement. This facility will have three fences surrounding it. The first outer fence will be 6 feet tall with barbed wire on the top. This fence will have cameras mounted every 250 feet and will not have an alarm built into it. The lack of alarm is meant to reduce nuisance alarms, while the fence still serves as a deterrent for basic adversaries and a delay for more advanced adversaries. This outer fence has a probability of detection of 0.1, which is considered the base value for "very low" detection. It serves as the boundary between the limited area and the off-site area. The remaining two fences separate the limited area from the protected area, with an isolation zone in between the two fences. These fences are topped with a single coil of concertina wire. All three fences are expected to provide 30 seconds of delay for adversaries with no tools and 10 seconds of delay for adversaries with tools.

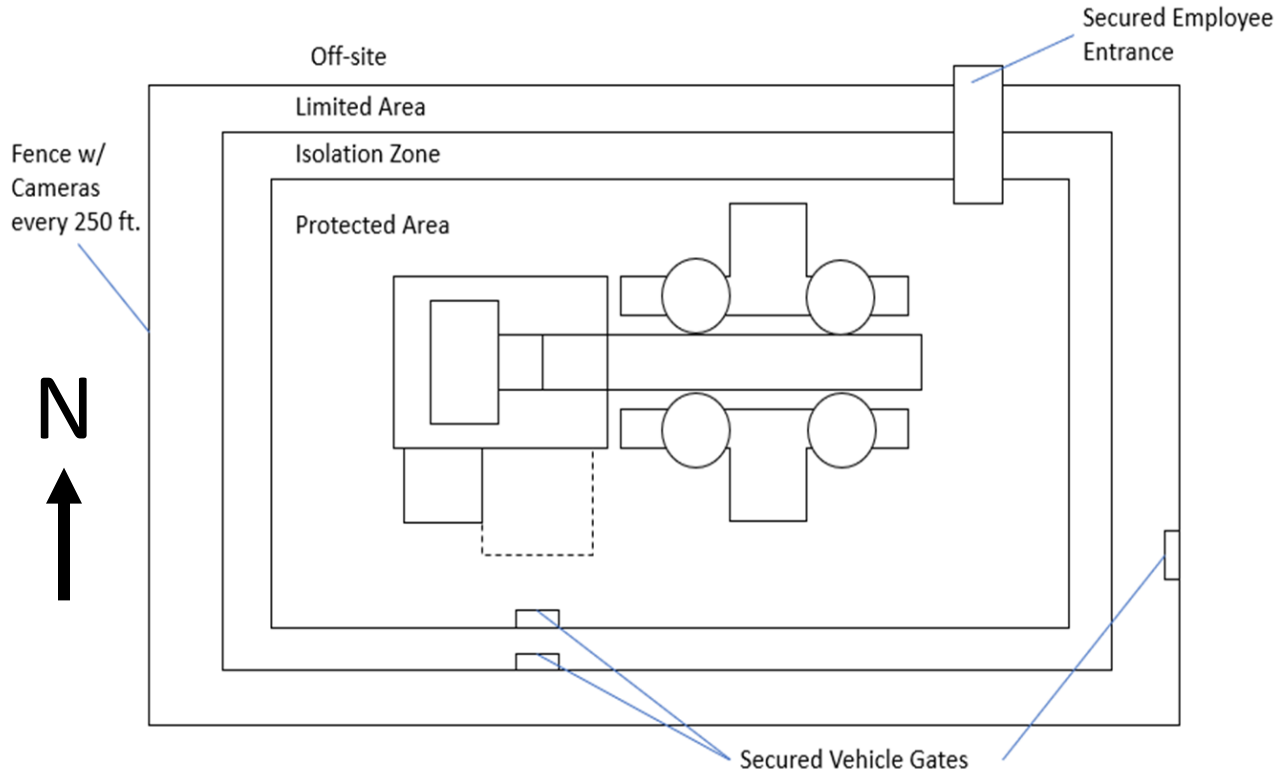


Figure 2. ESFR with fence placement.

A significant portion of the cameras and sensors will be present in the isolation zone. Like the outer fence, these inner fences will have cameras mounted on them. Each individual fence will have cameras every 500 feet but will have them set up in a way so that the isolation zone has a camera every 250 feet. This allows cameras to watch for someone tampering with another camera. The isolation zone itself is only ~10 yards wide, so having the cameras on two different fences will not affect the security of the isolation zone. These fences will also be equipped with taught-wire sensors, which will detect an adversary breaking through or climbing a fence. With the added sensors on these two fences, the probability of detection raises to 0.75, or "high" probability. Within this isolation zone, bistatic microwave sensors and active infrared banks

serve as a sort of "invisible fence" to detect intruders. The combination of both sensors is meant to reduce the number of nuisance alarms. Infrared banks, which are comprised of a source of infrared beams and a receiver, could be bypassed by an adversary either climbing on once of the receivers or crawling under the beams, while microwave sensors, which send out microwaves and detect changes in the reception of them, are incredibly sensitive to the point of producing large amounts of nuisance alarms. The combination of both types allows their weaknesses to be reduced, while providing all the benefits these devices have over other forms of sensors. Banks of sensors will be offset to avoid dead zones close to the microwave sensors, and detection zones will intersect each other to provide full coverage throughout the zone. The probability of detection for the sensors banks is 0.9, or "very high," and they provide no delay. To slow vehicles and on-foot adversaries, triple concertina wire will be placed on the ground next to the fence closest to the facility. This wire will provide a delay of 5 minutes for adversaries with no tools and 1 minute 30 seconds to an adversary with tools.

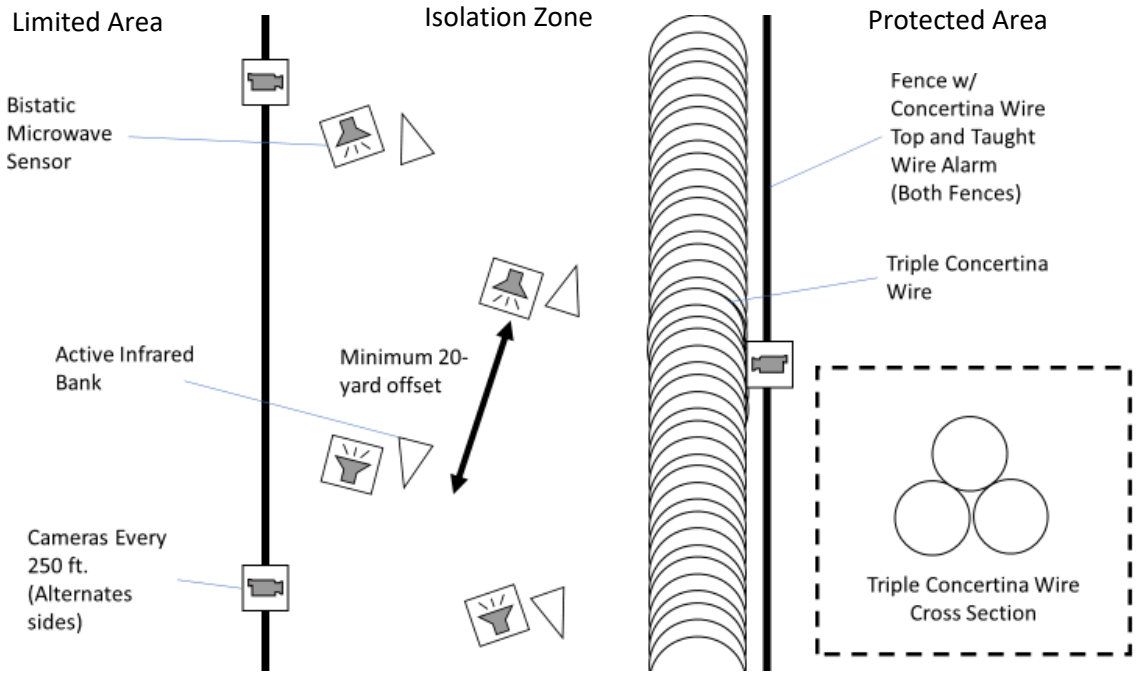


Figure 3. Diagram of the isolation zone security measures.

For maintenance or delivery vehicles to get through the fence line, they will have to pass through secured gate checkpoints. These checkpoints will contain a guard post, an electronically controlled gate, retractable columns to prevent vehicle ramming, and boulders or stone barricades to prevent cars from deviating from the path. The gates on the inner two fences will be in line with each other, while the outer most gate will not be lined up. This outer gate is placed away from the inner two to eliminate a straight path for an adversary to gain speed. Delay times for these secured gates are 3 minutes for adversaries without tools and 1 minute for adversaries with tools. Detection is harder to determine at a point like this, as it would depend mostly on recognition of a threat by any guards present. Although the guards will be highly trained, a safe probability of detection estimate for the gate is 0.5, or "medium."

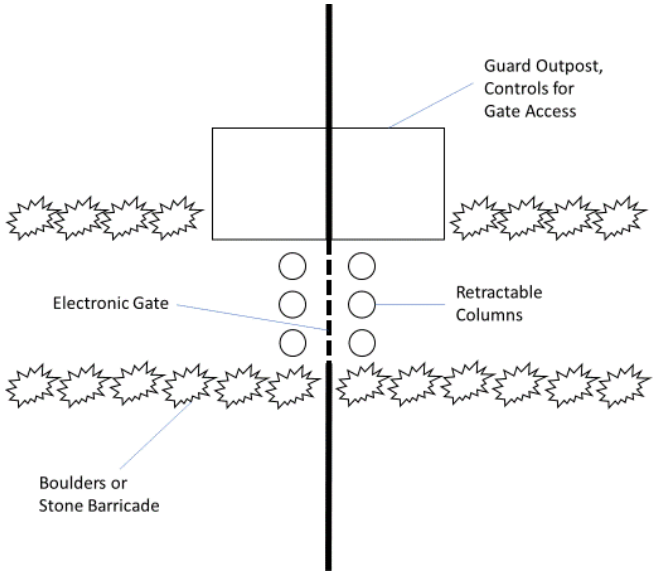


Figure 4. Example of a secured gate.

Employees will enter in from a specified entrance away from the vehicle entrance, and employee parking will be placed off-site. Employees will pass through a metal detector to get to the first secure access door. Both secure access doors will require a hand geometry scan and a card reader. This entrance building will also serve as the headquarters for guard personnel. Since this point will be where all three fences are closest to each other, a guard watch tower will be placed on the top of the building. Delay time is not considered for this building, as the fences attached would provide a much easier path of entry for the adversaries. Probability of detection is also not considered due to the devices present within the fence lines.

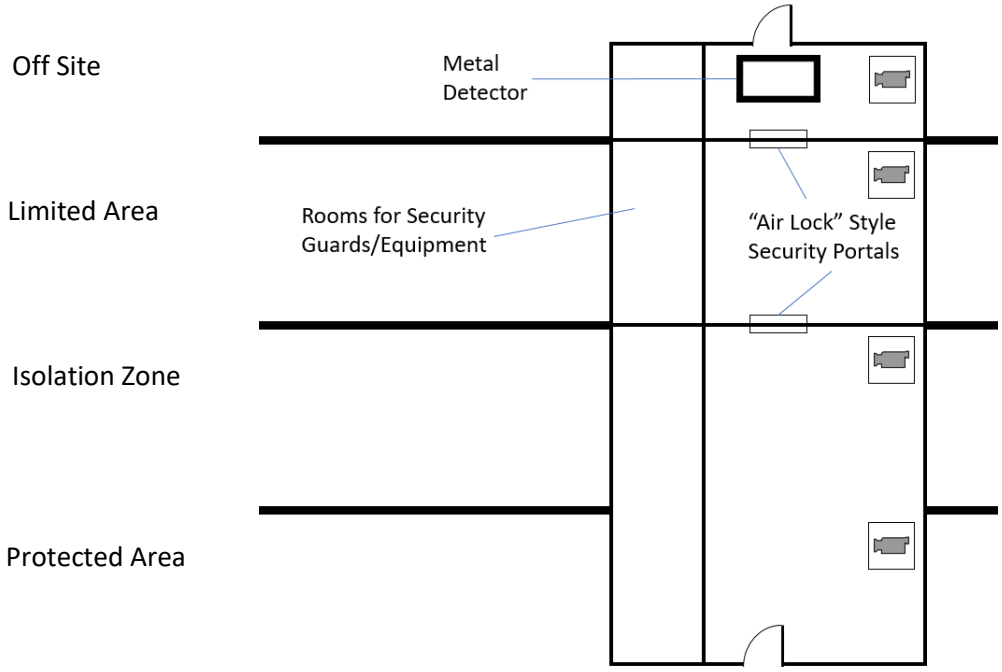


Figure 5. The employee entrance.

Spent fuel cask parking presents a lower value target than materials present inside the protected area. The cask parking fence will not be a chain-link fence like the perimeter fences, but a fence made of steel bars. These thicker bars will provide more security to the parking space. This area will also have an electronically controlled fence. This fence offers slightly higher delay times as the outermost fence, with the time delay without tools being 1 minute and with tools being 20 seconds. The probability of detection is also increased from "very low" to "low," bringing the probability to 0.25.

Moving onto the interior of the building, we start with the light water reactor spent fuel storage. The building will have personnel access doors to the parking area and to the fuel cycle facility. There will also be large garage-like doors next to these personnel doors in order to receive LWR fuel. The personnel doors will have hand geometry and card swipe to unlock them. The service doors will have controls inside the building. These doors will shut and lock when an alarm has been set off. Spent fuel will be stored in a spent fuel pool at the center of the room. The assemblies will be lowered in via crane, and the crane will lock up just like the service doors in the event of an alarm. Walls will be standard reinforced concrete and about one foot thick. This room will also have a security camera present to monitor for any strange activity.

The fuel cycle facility will be the largest of the rooms and will house three smaller rooms within it: the inert gas cell, the hot cell, and the storage pit. Fissile material is present in these three rooms, but it is not present in the rest of the room. There will be the previously mentioned doors that lead to the LWR storage, as well as two more secured doors, one on the west side and one on the north side. These doors are secured with hand geometry and card swipe access. Most of this room would not be of interest to adversaries. However, there will be an access port that connects this room with the inert gas cell so that material can get in and out of the inert cell. This access port will have two doors to keep the gas in the cell inert and to prevent any of that inert gas from filling up the workspace. These doors will be alarmed with magnetic switches that will go off if

forced open. Cameras will be present at several points in the room and in any smaller rooms not marked on the map. For this building, rebar reinforced concrete at 1 ½ foot thickness should suffice.

The storage pit will not be considered in this approach. The same material present in the hot cell is present in the storage pit, but the storage pit would be a much harder target to hit. Unlike the hot cell, where fuel assemblies will be out in the open, fuel assemblies in the storage pit will be stored in a deep, water-filled pool. These assemblies would only be accessible with a crane. The time it would take to acquire one of the assemblies from the pool will act as a deterrent.

The hot cell is where spent fuel assemblies have their spent fuel rods removed and replaced with new ones. Half of an assembly contains a significant quantity of nuclear material. Due to the high radioactivity of this room, all machines in this area will be remotely controlled from the fuel cycle facility. Like many of the machines in the fuel cycle facility, controls will lock up if an alarm is set off, and controls will require employee verification to use. The high levels of radiation will prevent the use of security cameras in this area, so other security measures will be put in place to detect access in the first place. The walls of the hot cell will be 2 ½ feet thick concrete with rebar reinforcement. Also in the walls will be a net of fiberoptic cables. These cables break when someone has broken through the wall, and the broken signal will set off an alarm.

The inert gas cell is where the actual reprocessing of the fuel takes place and serves as a valuable target for adversaries. Spent fuel is separated into uranium, plutonium, and fission products. Fuel rods are then refilled with nuclear material. The presence of loose nuclear material that can easily be transported out is what makes this area such a desirable target. The inert gas cell will have many of the same features the hot cell has: remote tools with alarm lockup, reinforced concrete walls, wall breach sensors. This area, due to the more complex nature of the process within it, may have some needed windows. These windows should be designed so that a human cannot fit through the window if all glass was removed. Since this cell is filled with an inert gas, adversaries will either need to minimize time in the cell or bring breathing apparatuses. The gas acts as a deterrent in this case.

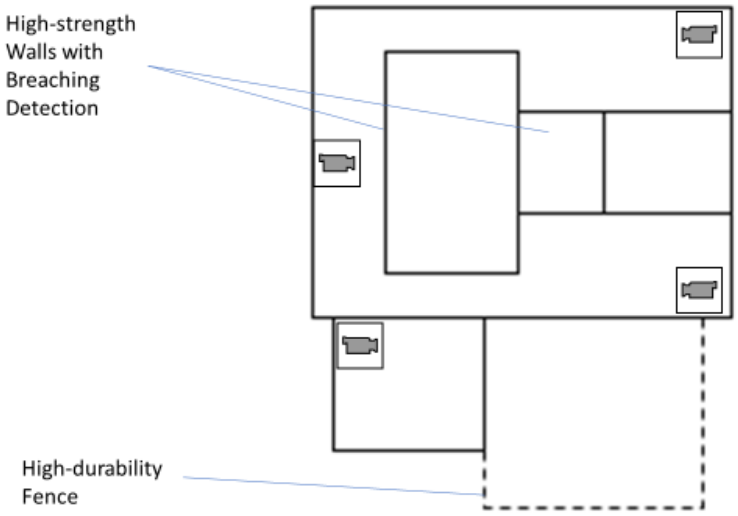


Figure 6. Interior and cask parking.

The fuel services facility will contain devices needed to help transition the fuel assemblies from the reactor to the fuel cycle facility. This area will be treated the same way the hot cell is treated. The only true difference in this area is the presence of cleaning machines instead of disassembly machines.

The reactor containment vessels at this plant are not seen as targets for theft. Large quantities of highly reactive sodium metal and the extreme amounts of radiation present make stealing from a breached reactor containment building extremely impractical.

All walls in this facility are assumed to have equal delay and detection. Though in reality thicker walls would take longer to get through, assuming a worst-case scenario would make assessment easier. The delay times for all walls in the facility are 5 minutes without tools and 1 minute with tools. The probability of detection for breaching these walls is “very high,” or 0.9.

There will be two guard patrol routes at this facility. The first route consists of two sets of four guards circling the fence separating the restricted area from the isolation zone in opposite directions. These guards will be fully equipped with compact rifles or submachine guns, flashlights, bulletproof vests, entry access cards, and radios. They will also be driving vehicles on their patrol. The second route requires a set of two guards to walk about the facility to check up on operations. They will have all the tools the previously mentioned guards have except for the rifles or submachine guns. Instead, these guards will be equipped with only pistols. Their pistol holsters will have a “holster switch” built into them so that if they draw their gun an alarm is set off. On top of the guards with set routes, there will be two guards at every gate for a total of six guards, and there will be eight guards stationed at the employee entrance area. Guards at the gates will be armed like those circling the perimeter, while the ones in the employee entrance will be armed like the building patrol. The guard stationed in the watch tower will be armed with a full-sized rifle.

Table 1. List of all delay times and probabilities of detection.

| Security Feature | Delay time without tools | Delay time with tools | Probability of detection |
|---|---|---|---|
| Outer Fence | 30 seconds | 10 seconds | 0.1 |
| Inner Fence | 30 seconds | 10 seconds | 0.75 |
| Microwave and Infrared Banks | N/A | N/A | 0.9 |
| Concertina Wire | 5 minutes | 1.5 minutes | N/A |
| Secured Vehicle Entrances | 3 minutes | 1 minute | 0.5 |
| Dry Cask Parking Area | 1 minute | 20 seconds | 0.25 |
| Walls | 5 minutes | 1 minute | 0.9 |

### *Physical Protection Plan Analysis*

To find weaknesses in the initial physical protection approach, we used a basic wargaming simulation of an actual attack based on the design basis threat. Concepts from the *Strategic Wargaming Series Handbook* were borrowed to aid us in how to perform a wargame [11]. Professor Robert Bean served as the "mediator" of the wargame. He would decide what was legal for the adversary to do under the design basis threat. Luke Tyree, a graduate student in nuclear engineering at Purdue University, served as the adversary. He is a Captain in the United States Army, which gave him valuable insight on how to get past the security plan. Christian Young served as the defending forces lead. He is the primary author of the security plan, and therefore was most fit to defend against an enemy.

The values from Table 1 are used qualitatively in the wargame. When the enemy team decided to do something that involves one of the listed items, the mediator used said values and the conditions of the attack at that moment to decide what happens next. For example, the delay time of a fence might prompt the mediator to allow the response force to reach the attackers before they got through the fence.

#### *Adversary Description*

The ten-man attack was broken up into three separate groups.

The first group consisted of two people stationed about 400m from the edge of the facility. One of the men was the team leader for the entire operation, while the other staffed a crew-serviced weapon. The crew serviced weapon was a type of heavy machine gun, providing the team with both range and ample suppressive fire. This team also guarded one of the two vehicles.

The second group consisted of three men. Their job was to provide a distraction for the roaming patrols in the limited area. This team had basic tools for breaching fences and was armed with basic assault rifles and body armor.

The third team consisted of the remaining five men. This team was responsible for the theft of the material from the facility. One of the men operated the second vehicle, which was rigged with explosives to become a car bomb. The other four had more sophisticated assault rifles, tools to get through fences, and shaped charges to get through doors and walls.

*Attack Simulation*

The adversaries began their attack on a clear, sunny day to increase visibility. The attack began when the distraction team breached the northwest corner of the fence. They made their way to the limited area and broke into the isolation zone with no concern about being detected. It was here that taught-wire and microwave sensors picked up an intruder, triggering an alarm. The two patrol units were then dispatched to the area of the alarms. It should be noted that the initial attackers were far enough away from the secured employee entrance that the guards present would not be able to see them approach and breach the area.

The concertina wire in the isolation zone slowed the initial attackers down enough that they had to retreat back to the limited area to fight off any response force. One of the two response vehicles was able to make it, but the other was caught by suppressive fire from the crew-serviced weapon. This group was considered unable to contribute for the rest of the simulation.

Once the distraction team was engaged with the patrols, the final team started their attack. They breached the initial fence and a car bomb was driven to the second secured vehicle gate. Although the alarm caused barriers to go up in front of the gate, the bomb was assumed to be powerful enough to destroy both fences and neutralize all guards in the area. The remaining four in the team used breaching charges to break open any doors or walls in between them and the inert gas cell. The two guards present in the building were neutralized with little effort from the attack team. The team was able to gather a significant quantity of nuclear material. They escaped to the location of the crew-serviced weapon, and those remaining escaped from the facility. It is assumed that local law enforcement would not have made it in time to stop the escape.

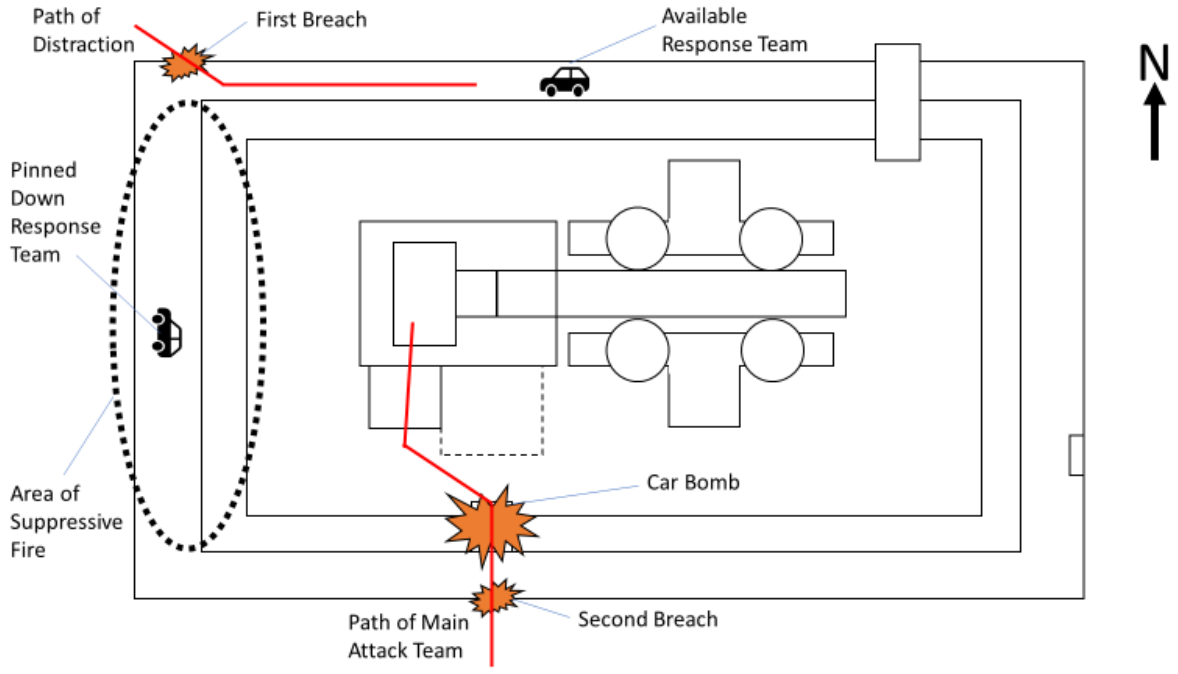


Figure 7. Diagram of the simulated attack.

## Conclusions

### *Potential Changes and Considerations*

When designing the physical protection plan for this facility, a lot of emphasis was put on detecting an adversary taking a stealth approach. While many methods of detection were placed within the isolation zone and protected area, not enough was done in the limited area, especially considering that an attacker with no desire for stealth got through the limited area without detection. Additional detectors in this area would help detect an enemy sooner, but at the cost of increased nuisance alarms and monetary cost.

Guard response was lacking severely. One of the patrols was pinned down early in the assault, and although other guards were present at the facility there was no extra response force set up. There are many ways to remediate this. First and foremost, increasing the number of guards present on patrols and in buildings will increase the likelihood that an adversary would be stopped in their attack. There were simply too few guards at this facility to handle this kind of attack. Second, better entrances and exits for guards will allow them to move around the facility. The group that was pinned down by the machine gun may have been able to escape to the protected area if there had been more than one secured entrance to this zone. Changes like increasing the number of secured entrances will allow guards to adapt more fluidly to the changing situation. Finally, strict defensible positions will help guards defend targets more effectively. When the two building guards were met with the attacking force, they did not have proper defense and were quickly neutralized. Guard posts inside and outside of buildings will give guards places to engage targets while still staying relatively safe. Guard towers will also give guards more defensible positions and will add to the detection capabilities of this plant, especially if guard towers were placed inside the limited area. A more thought out conduct of operations would also help in neutralizing the threat once it has been detected.

Besides the clear flaws in the security approach, there are other ideas that should be addressed in future iterations of analysis. Due to the time constraints of this paper, only one wargame simulation was run. Multiple simulations should be done with continuously improving approaches to get the best security approach possible.

The first topic to discuss is the lack of boundary dimensions. For the first iteration it was assumed that the actual size of the limited area and protected area would not be needed. While it proved to be irrelevant for the simulated attack, the size of each area could greatly influence other future attacks. Were this plant to undergo more iterations, values would be added.

Similarly, time delays on each component were not present, so it became unclear at times what would delay the attackers and what would not. This is not easy information to get access to, though rough estimates should be considered for future iterations.

Location of the plant should be considered in the future. For our simulated attack, we assumed that there would be a high ground area for the mounted gun to sit on. That could have easily been remedied by stating the location of the plant. Other terrain factors may influence future simulated attacks. In addition, the amount of people in the surrounding area would influence the response time of the local police and could lead to an attack force being detected before the attack even began.

Finally, some tools and weapons were left out of this initial analysis. Access to rocket launchers or anti-vehicle tools would provide both the adversary and the security force a wide range of new tactics. Jamming capabilities on both ends would also change the dynamics of the attack. Force multipliers, like remote operated weapons, would help increase the firepower of the defending team without having to hire more guards.

### *Final Thoughts*

While a real physical protection plan would require multiple iterations of the design and analysis steps, our group was able to explore the fundamental basics of nuclear security. We took the Example Sodium Fast Reactor developed by the Generation IV International Forum and used devices suggested by *The Design and Evaluation of Physical Protection Systems* to secure it. Once we had an initial plan, we simulated a wargame to find weaknesses, and applied concepts from *Vulnerability Assessment of Physical Protection Systems* to remediate these issues. Now that this process has been done publicly on a base level, others can use this as an example of the security assessment process to learn more about the field of nuclear security.

## Authors

Christian Young is a current undergraduate student in nuclear engineering at Purdue University. He is part of the Summer Undergraduate Research Fellowship program, for which this paper was written. After he graduates in 2020, Christian plans to enter graduate school to pursue a career in academia.

Dr. Robert Bean graduated from Purdue University in 2003 with a Ph.D. in Nuclear Engineering. He then worked in safeguards measurements and safeguards design at the Idaho National Laboratory, including a two-year term as a Technical Advisor in safeguards and radiation detection research for the U.S. National Nuclear Security Administration. In 2013 he returned to Purdue as a professor in Nuclear Engineering and as the director of the Nuclear Engineering Radiation Laboratories.

## References

[1] Bari, R., Peterson, P., et al. 2009. Generation IV International Forum, *PR&PP Evaluation: ESFR Full System Case Study*, Final Report

[2] Bathke, C., et al. 2012. Nuclear Technology, *The Attractiveness of Materials in Advanced Nuclear Fuel Cycles for Various Proliferation and Theft Scenarios*, Vol. 179, Issue 1.

[3] Bunn, M. 2013. Belfer Center for Science and International Affairs, *Strengthening Global Approaches to Nuclear Security*

[4] Garcia, M. L. 2007. *The Design and Evaluation of Physical Protection Systems, 2nd Edition,* Butterworth-Heinemann, Burlington, Massachusetts, United States of America

[5] Garcia, M. L. 2005. *Vulnerability Assessment of Physical Protection Systems*, Butterworth-Heinemann, Burlington, Massachusetts, United States of America

[6] International Atomic Energy Agency. 2009. *Development, Use, and Maintenance of the Design Basis Threat*

[7] International Atomic Energy Agency. 2011. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/25/Revision 5

[8] International Atomic Energy Agency. 2013. *Nuclear Security Series Glossary*

[9] United Nations, 2005. Annex to General Assembly resolution 59/290, *International Convention for the Suppression of Acts of Nuclear Terrorism*

[10] United States Army War College. 2015. *Strategic Wargaming Series Handbook*