Overview of Security Plan for Offshore Floating Nuclear Plant

Proceedings of the 2016 24th International Conference on Nuclear Engineering
ICONE24
June 26-30, 2016, Charlotte, North Carolina

ICONE24-61029

OVERVIEW OF SECURITY PLAN FOR OFFSHORE FLOATING NUCLEAR PLANT

Vincent Kindfuller*
Neil Todreas
Jacopo Buongiorno
Michael Golay
Department of Nuclear Science and Engineering
Massachusetts Institute of Technology
Cambridge, Massachusetts, 02139
vjk@mit.edu

Arthur Birch
Thomas Isdanovich
Ron Thomas
ECSI international, Inc.
Clifton, NJ 07012

Harvey Stevens
Stevens Associates, Inc.
Red Bank, New Jersey 07701

ABSTRACT

A new Offshore Floating Nuclear Plant (OFNP) concept with high potential for attractive economics and an unprecedented level of safety is presented, along with an overview of work done in the area of security. The OFNP creatively combines state-of-the-art Light Water Reactors (LWRs) with floating platforms such as those used in offshore oil/gas operations, both of which are well-established technologies which can allow implementation on a time scale consistent with combating climate change in the near future. OFNP is a plant that can be entirely built within a floating platform in a shipyard, transferred to the site. OFNP eliminates earthquakes and tsunamis as accident precursors; its ocean-based passive safety systems eliminate the loss of ultimate heat sink accident by design. The defense of an OFNP poses new security opportunities and challenges compared to land-based plants. Such a plant can be more easily defended by virtue of the clear 360 degree lines of sight and the relative ease of identifying surface threats. Conversely the offshore plant is potentially vulnerable to underwater approaches by mini-submarines and divers. We investigate security considerations of the OFNP applicable to two potential plant options, an OFNP-300 with a 300 MWe reactor, and an OFNP-1100 with an 1100 MWe reactor. Three innovative security system approaches could be combined for the offshore plant. The first is a comprehensive detection system which integrates radar, sonar and unmanned vehicles for a long distance overview of the vicinity of the plant. The second approach is the use of passive physical barriers about 100 meters from the plant, which will force a fast-moving power boat to lose speed or stop at the barrier allowing the plant security force more time to respond. The third approach takes advantage of the offshore plant siting and the monthly or biweekly rotation of crew to reduce the total on-plant and on-shore security force by using the off-duty security force on the plant as a reserve force. Through the use of these approaches, the OFNP-300 should be able to achieve a similar security cost (on a per Megawatt basis) as land-based plants of similar or somewhat larger power rating. Due to non-linear scaling of cost, the security cost of the OFNP-1100 has the potential to be reduced significantly compared to its land-based equivalents.

1 Introduction

Despite the promise of the Nuclear Renaissance in the 2000s, rising capital costs, delays in the construction of currently ordered nuclear plants and the very low cost of natural gas have combined to severely reduce the number of ordered new nuclear power plants in the US as well as cause the closing of existing plants due to high cost of upgrading and repair of technology. The concept for the Offshore Floating Nuclear Plant (OFNP) has several advantages relative to these issues, including the reduction in expensive structural concrete needed, the use of the ocean as an infinitely available ultimate heat sink, and, perhaps most appealingly in the wake of Fukushima, inherent protection from

*Address all correspondence to this author.

FIGURE 1. OFNP-300 CYLINDRICAL-HULL DESIGN

earthquake and tsunamis. Additionally offshore siting can eliminate the need for evacuation and minimize the degree of land contamination in the event of a radioactive release. The OFNP employs a standard nuclear plant on a cylindrical-hull platform of the type commonly used in oil platforms, as shown in Figure 1. Two designs are being developed in parallel: the OFNP-1100 based on a class 1100MWe reactor such as the Westinghouse AP 1000 reactor and the OFNP-300 based on a class 300MWe reactor such as the Westinghouse Small Modular Reactor [1]. Both OFNPs will be sited somewhere between 10 and 12 nautical miles offshore (the 10-mile minimum ensures an emergency planning zone with zero residents, the 12-mile maximum is the territorial waters limit), in water-depth of at least 100 meters.

In the wake of 9/11, there was significant scrutiny on the security of nuclear plants, as the specter of terrorists destroying a nuclear plant or stealing nuclear materials was brought into focus. The offshore siting of the proposed OFNP offers some advantages, as well as some disadvantages, compared to the security of a conventional, land-based plant. One major cost driver for conventional plants is the large size of the security force to meet the more stringent regulations that have been imposed over the years since 9/11 and the limited response time available to mitigate a threat. Consideration of security at this initial stage of offshore floating plant design helps to lower security costs and prevent the necessity of having to design security features into an already designed platform. Ensuring an adequate level of security is a major design objective for the OFNP concept. The security plan for this paper applies to both the OFNP-300 and OFNP-1100, with the various aspects of the plan identified for both. There are two goals for the security plan. The first is to be able to detect and assess a threat at a maximum distance and repel an attack on the plant, and the second is to minimize costs as possible. The requirements we have suggested here which the security plan must meet are both those imposed by governmental regulation and those adopted for investment protection. For governmental regulation we tentatively adopt those of the US Nuclear Regulatory Commission which would be necessary for siting in United States waters and serve as an initial surrogate for regulations which might be imposed by the host country of an international offshore site. This paper first presents the security requirements which must be met for current, deterministically-based USNRC regulations and those that have been selected for investment protection. The central distinction between these categories is that the NRCs requirements derive from its statutory authority which is limited to requiring protection against significant core damage and spent fuel sabotage, actions which pose risk to public health and safety, while the second category stems from the desire that the plant can continue to operate reliably and generate revenues for its owner. The paper then explains the proposed security features already selected for the OFNP plant and those key areas such as refueling and maintenance which will definitely impact achievement of these security requirements but for which insufficient design work has been performed to date to enable the security approach to be specified. Finally, the paper explains security-related cost-saving measures that will be implemented and compares an estimated final cost of a postulated set of security features on a per Megawatt basis to a conventional, land-based plant.

2 Offshore Floating Nuclear Plant Concept

MIT is developing two OFNP designs in parallel which would be used in different markets: the OFNP-300 and OFNP-1100, designated according to their electric power rating [1]. The OFNP-1100 is based on a class 1100-MW reactor such as Westinghouses AP1000 [2], which is already NRC design certified and being built in the U.S. and China. The OFNP-300 is based on a class 300-MW reactor, such as Westinghouses Small Modular Reactor (WSMR) [3]. In both cases, the floating structure chosen to house the nuclear plant is a cylindrical hull-type platform that shares many of its characteristics with platforms used in the offshore oil and gas drilling industry. The cylindrical hull design offers substantial dynamic stability gains at the scale the OFNP is designed for, when compared to other offshore platform

TABLE 1. OFNP PLATFORM CHARACTERISTICS

Parameter	OFNP-300	OFNP-1100
Hull/skirt Diameter(m)	45/75	75/106
Draft(m)	48.5	68
Total Height (m)	73	108
Main Deck Height(m)	12.5	34
Displacement (tonnes)	~115,500	~376,400
Structural Concrete (ton/MWe)	~2	~4 *

* Compare to ~69 ton/MWe for the AP1000 plant

TABLE 2. QUALITATIVE ADVANTAGES OF OFNP WITH RESPECT TO LAND-BASED NUCLEAR POWER PLANTS

Site	On-Land	Offshore
Licensing	Site specific (ground and seismic requirements)	Standardized (site-independent design)
Construction	At site, requiring enormous amounts of concrete resulting in high cost and frequent schedule delays	In centralized shipyard; structural concrete is virtually eliminated
Ownership and Operations	Domestic utility owns and operates the plant with domestically trained workforce	International utility could own and operate a worldwide fleet of plants, with crews that receive standardized training and operate in semi-monthly shifts (onboard living quarters)
Safety	Passive safety (new plants); evacuation possibly needed in case of severe accidents	No loss of heat sink; no earthquake and tsunami vulnerability; superior defense in depth; no resident population evacuation needed
Plant lifetime	60 years, all at one site	60 years; can track most profitable markets with minimal local infrastructure (plug-and-play approach)
Decommissioning	At site, decade-long project	Immediate return to green field; decommissioning in shipyard

designs, such as semi-submersibles or floating barges [4–7]. The cylindrical hull design also enables the reactor and containment to be located at an elevation below the waterline, which enhances physical protection from plane crashes and collisions with ships, while also making it easier to access the ocean heat sink. The OFNP balance of plant includes a standard Rankine cycle, a step-up transformer, both located onboard the platform, and several submarine AC cables to transmit the electric power to the grid on land [8]. Summary dimensions for the OFNP-300 and OFNP-1100 platforms are reported in Table 2.

The design philosophy of the OFNP is to:

(i) Use only proven and qualified materials and components, for both the nuclear island and the floating platform. This reduces development and licensing costs and schedule, and maximizes reliability in operations.

(ii) Design the plant for modular, streamlined construction in existing shipyards. The platform hull, the nuclear island and the platform topside can be constructed independently (possibly at different shipyards), and then assembled at a single shipyard. It is the shipyard capabilities that drive the design of the plant, not vice versa. This reduces the need for re-design during construction, and ultimately reduces the construction schedule and uncertainty.

(iii) Systematically integrate multiple functions into single systems, structures and components that are not safety related. This makes the plant more compact and efficient without introducing common-cause failure mechanisms in safety systems. For example, an annular skirt is attached to the bottom of the platform hull to function as an oscillation dampener, but also to provide extra buoyancy during transportation of the platform.

More information on the OFNP design can be found in Reference [9]. The OFNP concept affords several advantages and flexibilities in construction, operations, safety and decommissioning that are not possible with traditional land-based nuclear power plants, as described in Table 2. This paper focuses on the OFNP security principles and their implementation in the OFNP design.

3 Overview of Challenges

Although there are some similarities, for the most part the security situation of a land-based plant is very different from that for an offshore plant. The underwater dimension of an offshore plant creates a new challenge for defending the OFNP, as does the possibility of collisions with large vessels and the need to prevent sinking. On the other hand, the clear 360 degree lines of sight and relative ease of detecting and identifying surface threats at distances can help afford adequate response time to mitigate the threat. The most analogous offshore installation is an oil platform, but due to the relative lack of importance oil platforms place on security compared to that which is required for a nuclear plant, it is not an entirely informative comparison [10]. Rather, two more useful security plans to examine are those around ports and those around naval vessels in port. While both have their own differences from the security needed for this reactor plat-

form, nonetheless, a comparison is instructive.

Both ports and naval vessels utilize floating booms to encircle vulnerable areas and create a standoff distance between them and a potential attacker. In addition, both utilize detection measures to attempt to identify potential threats before they become threats. The responses of both of these to two specific threats that are unique to an offshore environment are instructive. The first unique threat is that of underwater attack, such as a diver or a submersible. Both ports and naval vessels use sonar to detect a diver or other underwater threat. In addition, both use underwater netting to deny access for divers to vulnerable areas, whether that be the hull itself for a naval vessel or a restricted part of the port. For ports and naval vessels alike, the response to the second unique threat, a potential ship collision threat, is, first, to detect the vessel, identify, communicate and warn away the approaching vessel, then, second, attempt to intercept and stop it, and or use barriers to deflect or halt it, and, third, design for collision resistance. A similar approach will be developed for the OFNP and addressed more fully in the future.

Security costs make up an important proportion of the cost for conventional, land-based reactors, and the OFNP should be designed with security in mind in order to reduce unnecessary costs. Hardware costs are one-time costs, although the necessities of maintenance and replacement will add a small recurring cost to that total, and both those one-time costs and the maintenance costs are relatively small compared to the cost of maintaining the security force. This will be even truer for an offshore plant, as, just as with an oil platform, the costs for an employee on the platform will be significantly higher than for an equivalent employee who works on land. Therefore, personnel requirements will be the driver of total security cost. Thus, as much as possible, increased hardware usage should be leveraged to decrease personnel requirements, and thus decrease total life cycle cost.

4 Development of the Security Plan

The primary goal of the security plan is to protect the plant from attack, preventing either damage to the containment and radiological release or loss of control of the reactor. We recognize that potential attackers could have other goals in mind, but for this work we restrict ourselves to these. In proposing the security plans requirements and its response elements, it is useful to structure its development along the following phases:

(i) Establish the design basis threat (DBT)
(ii) Identify targets and target sets
(iii) Draft adversary attack scenarios
(iv) Develop a preliminary protective strategy and, from this, imbue the design with security components to support the strategy
(v) Finally demonstrate the ability of the strategy to defend against the DBT.

This structure is consistent with US regulatory philosophy and for the purposes of this paper we adopt it. However we anticipate that refinements are possible particularly from our future use of risk informed arguments. In addition, in siting in countries other than the US we recognize that other regulations will apply, although we feel that NRC regulations stand as a useful preliminary stand-in for potential host countries regulations.

We present the following preliminary response to the first five phases as an illustrative example based on the premise that USNRC security regulations will be met for our OFNP:

4.1 The Design Basis Threat

The NRC Design Basis Threat requires that the security force must be able to deal with a hostile well-trained force attacking from one or more directions, supported with inside assistance, and equipped with military grade weapons, equipment and vehicles, or a vessel-borne bomb attack. An essentially similar requirement should apply for offshore plants. The precise specification of the NRC DBT used for land-based reactors is classified, but would need to be also identified for an offshore plant. The general description cited above is sufficient for this preliminary plan.

The DBT definition also includes definition of the adversaries, i.e. Threat Actors– There are three major categories of potential threat actors a hostile state, a sub-state or terrorist group, and an individual. Each may have different motivations, equipment, knowledge and training, and each must be considered in the security strategy. A hostile state threat represents a conventionally armed military force directly supplied by an organizing and directing countrys government. According to NRC regulations, nuclear plants do not have to defend against an attack by an enemy of the state, by which is meant a hostile state attacking with full-scale conventional forces. However the Design Basis Threat which plants must be equipped to defend against includes the possibility of an attack by well-equipped attacking forces with boats and equipment, such as a unit of a states special forces. A sub-state actor refers to a terrorist or guerilla group, operating officially outside of the aegis of any state. Their equipment and organization can vary from non-aggressive protestors to well-trained and equipped militants. This threat should be the main focus of security plans, as it is more likely than a hostile state attack, and more potentially damaging than an attack by an individual. An individual attack is an attack by a single person, acting independently. This may be no more than a single person without a plan, who cannot appreciably affect plant operations. However, it is also possible that an individual attacker could be an employee of the plant, who decides to damage the plant in some manner from the inside. As an insider, such a person has the opportunity and knowledge to inflict massive damage on a plant.

TABLE 3. THREAT AXES

Threat Origin	Land-based	Moored on Surface	Underwater
Hostile State	(i) Direct Attacks (a) Ground Assault (b) Bombing (c) Surface Naval Strike (from river) (ii) Attacks on Infrastructure (a) Cyber Attack (b) Nuclear Materials in Storage or Transit (c) Siting-Specific Secondary Threats (e.g. dams, levees)	(i) Direct Attacks (a) Boarding (b) Bombing (c) Surface Naval Strike (d) Sub-surface Strike i. Submarine/Mini-sub ii. Divers (ii) Attacks on Infrastructure (a) Cyber Attack (b) Nuclear Materials in Storage or Transit (c) Mines (d) Supply Lines	(i) Direct Attacks (a) Air-Launched Torpedo (b) Sub-surface Strike i. Submarine/Mini-sub ii. Divers (ii) Attacks on Infrastructure (a) Cyber Attack (b) Nuclear Materials in Storage or Transit (c) Mines (d) Supply Lines
Terrorist and Non-State Actors	(i) Direct Attacks (a) Ground Assault (b) Suicide Bomber i. Truck Bomb ii. Airplane/Drone (c) Standoff Attack (Rockets/Mortars) (ii) Attacks on Infrastructure (a) Cyber Attack (b) Nuclear Materials in Storage or Transit (c) Supply Lines (d) Siting-Specific Secondary Threats	(i) Direct Attacks (a) Boarding (b) Suicide Bomber i. Fast Boat ii. Diver iii. Airplane/Drone (c) Standoff Attack (Rockets/Mortars) i. Small Boat ii. Shore Based (d) Intentional Collision (ii) Attacks on Infrastructure (a) Cyber Attack (b) Nuclear Materials in Storage or Transit (c) Supply Lines (d) Mines	(i) Direct Attacks (a) Suicide Bomber (b) Torpedo i. Air-Launched ii. Sub-launched (c) Diver (ii) Attacks on Infrastructure (a) Cyber Attack (b) Nuclear Materials in Storage or Transit (c) Supply Lines
Insider	(i) Direct Attacks (a) Sabotage i. Disruption of Operations ii. Damage iii. Radioactive Release (b) Explosives i. Disruption ii. Damage iii. Radioactive Release (ii) Secondary/Indirect Attacks (a) Cyber Attack (b) Bomb Threat (c) Information to attackers	(i) Direct Attacks (a) Sabotage i. Disruption of Operations ii. Damage iii. Radioactive Release (b) Explosives i. Disruption ii. Damage iii. Radioactive Release (ii) Secondary/Indirect Attacks (a) Cyber Attack (b) Bomb Threat (c) Information to attackers	(i) Direct Attacks (a) Sabotage i. Disruption of Operations ii. Damage iii. Radioactive Release (b) Explosives i. Disruption ii. Damage iii. Radioactive Release (ii) Secondary/Indirect Attacks (a) Cyber Attack (b) Bomb Threat (c) Information to attackers

4.2 Targets (Threat Axes)

Table 3 lists the potential ways in which different attacker forces may attempt to attack a nuclear power plant, and how the attempts may vary between land-based, floating, and submerged plants.

4.3 Attack Scenarios

Here we identify those points of plant vulnerability around which potential attack scenarios might be developed. Attackers have the choice of several specific locations within the reactors operational facilities that they may choose to target. An attacker may target different sections of the plant depending on the attacks motive- whether it be plant destruction, disruption, capture or creation of a nuclear incident. Table 4 gives an overview of points an attacker may target in a nuclear plant, based on the goals of an attacking force.

Destruction of the plant would entail some focused attack on the platform and structure. Disruption of the plant would result from the attacking force targeting an operational system, such as coolant pipes, to attempt to create a large Loss of Coolant Accident and force the plant to lose cooling capability and potentially release radioactive material. Alternatively, they may target safety systems, such as redundant coolant injection systems, or balance of plant systems such as the turbine steam system, to force the plant to shut down without risk of nuclear release. An attacker could also attempt to capture or destroy the control room, which could allow them to gain control over the plant. This could be to force an intentional nuclear accident in the plant, or to merely hold the plant for ransom or political goals, as has been done for both oil platforms and cargo ships in the past. Finally the attackers goal could involve focus on those systems or structures housing operating nuclear fuel or spent nuclear fuel.

4.4 Requirements upon which to develop a preliminary protective strategy

The USNRC regulates security for terrestrial nuclear electricity generating plants principally through the requirements of document 10CFR Part 73 with some supplements through clarifications provided by Regulatory Guides and research results by the NUREG report series. While it is possible that NRC security requirements may be developed for innovative new reactor concepts particularly ones such as this offshore floating plant, at this time we will base our design on the existing principal terrestrial security requirements. Although NRC regulations may not be adopted in their entirety for the OFNP, the basic outline serves as effective preliminary guidance to OFNP security. Those that principally determine the protective strategy which we will adopt are as follows. In addition we add investment protection requirements as noted below.

TABLE 4. ATTACKER PLANT TARGETS FOR ATTACK GOAL

Target	Destroy	Disrupt	Capture	Nuclear Incident
Body of Building	X			
Safety Systems		X	X	X
Operational Systems		X		X
Control Room		X	X	X
Shore site		X	X	
Containment Structure	X			X
Spent Fuel Pool				X
Power Transmission		X		
Flotation Capability	X			

Regulatory requirements:

(i) The plant must be able to successfully respond to the NRC Design Basis Threat which has been defined in 4.1

(ii) The plant must be able to deal with an insider attack with knowledge of the plant who is either passively or actively aiding outside attackers. Although such an insider does not change the potential methods of attack of any given hostile group, it adds the complication that the attacker will know information about the layout and security of the plant, and will be able to rely on a disruption of security by the insider.

(iii) The plant must implement a comprehensive insider mitigation program including items such as pre-employment screening, psychological evaluations, drug/alcohol testing, and supervisor behavioral observation.

(iv) The offsite force response to relieve the onsite security force from an attack by an adversary force must be timely, for example within a half hour.

(v) The plant must control the entry of personnel/vehicles within the protected area (which we later label the controlled access area)

Investment Protection requirements:

(vi) Ship collision - Mitigate the risks caused by a potential ship

TABLE 5. SECURITY RESPONSIBILITIES

	Host-Nation	OFNP Security Team
Air	(i) Military Aircraft (ii) Commercial Aircraft (iii) Missiles	(i) Remote Control Drones (ii) Light Planes (iii) Helicopters
Surface	(i) Large Tankers (ii) Military Vessels	(i) Non-military Surface Vessels
Sub-Surface	(i) Large Submarines	(i) Mini-subs (torpedoes) (ii) Divers

collision, particularly a collision with a large oil or LNG tanker

(vii) Mitigate damage and risks caused by detonation of explosives near the plant

4.5 Preliminary Protective Strategy

The initial step in developing this strategy is to identify which security threats are the responsibility of the plant security forces to counter and which revert to the host nation, effectively its military capability to respond to. This division of responsibilities for Air, Surface and Subsurface launched threats is defined in Table 5.

The subsequent elements of the strategy and security components will be presented in the balance of this paper.

5 Features Impacting Security Plan

The OFNP -300 and OFNP-1100 employ a cylindrical-hull type design, taken from oil platform best practices. The dimensions of the OFNP-300 and OFNP-1100 are reported in Table 2 in Section 2. The Central Alarm Station (CAS) will be housed in the hull on the deck level adjacent to one of the two access points to the platform. Figures 2 and 3 demonstrate the internal layout of the cylindrical-hull platform.

The containment itself will be situated in the center of the platform, 20 meters below the waterline in the OFNP-300 and at the waterline for the OFNP-1100. The containment will be surrounded by a dry area in an inner hull, with a flooded area further outboard from the core. Non-vital components such as the steam system and turbines will be sited in the turbine hall above the waterline, while all safety components will be sited directly above and around the reactor compartment and beneath the waterline. Due to the watertight nature of levels below the waterline, the risk of flooding is judged to be less limiting than risk of attack

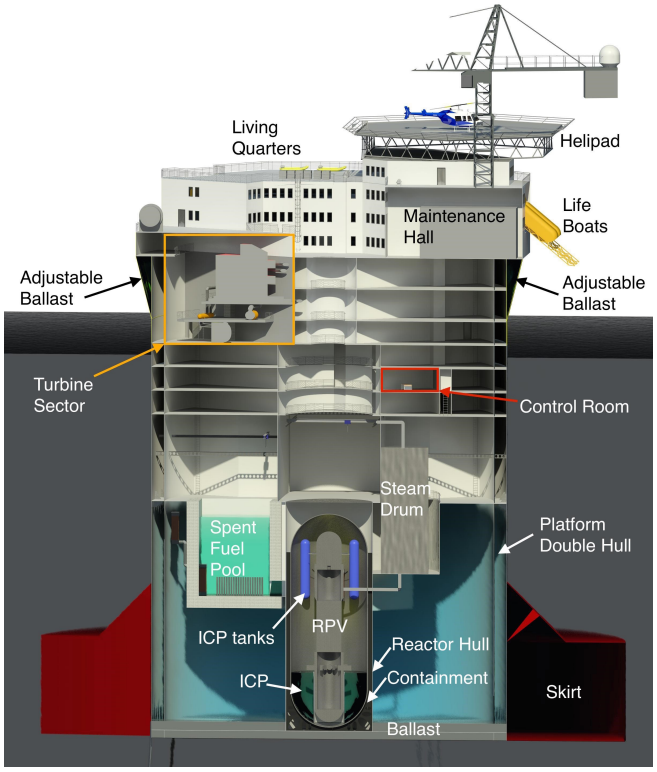

FIGURE 2. INTERNAL LAYOUT OF OFNP-300

(by explosives, plane or drone crash or other methods) on components on the upper levels. Therefore, safety components are located below the waterline, although for redundancy important safety components will be duplicated at different levels and sides of the platform. The control room will be on Level 5 on both the OFNP 300 and the OFNP 1100, only accessible directly from the upper levels and with no direct access between the control room and any of the operating components in this example.

In order to ensure watertight integrity in case of a breach of the hull, the platform will be divided into six sectors, each of which are entirely isolated from the others to ensure that a leak in one will not compromise the rest of the platform. In addition, the entire platform below level 3 will be watertight, with watertight doors on ladder-ways and internal access points. In order to ensure personnel safety in case of a serious casualty, each section has two access points to upper levels, in accordance with safety best practices. All of the watertight doors will be alarmed, monitored and access controlled from the CAS to insure they are secured. These features, as well as ensuring watertight integrity, will also help prevent unauthorized access to sensitive areas.

Personnel quarters will be on the deck of the platform, as will all personnel support facilities. A helicopter pad for im-

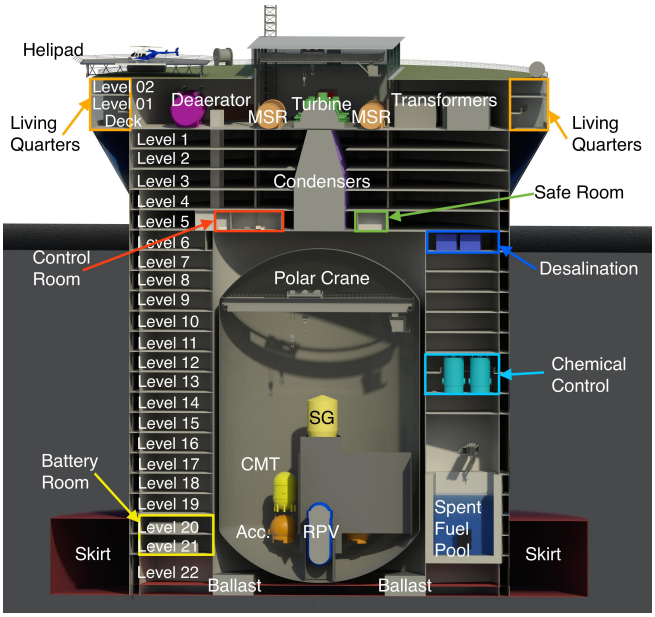

FIGURE 3. INTERNAL LAYOUT OF OFNP-1100

portant transport will also be situated on top of the platform, although routine personnel and materials transfer will take place by ship to a personnel transfer station on the hull of the platform. The required personnel on the platform for operations and associated maintenance will be established after the specific reactor plant design has been established. The plant will operate on a three week on, three week off schedule, consistent with oil platform practices, and there will be one personnel transfer every week.

Along with the platform itself, the operation of the plant will require a Secure Shore Support Facility to support functions that cannot be handled on the platform such as personnel security screening and food and equipment loading for transfer to the platform. The primary function of the shore facility will be to provide a place at which the supply ship can take on passengers and supplies, while being screened by security. In addition, the shore facility will also be the place at which the electric cables from the platform reach the shore, and the location of the Secondary Alarm Station (SAS) required by Nuclear Regulatory Commission regulations.

The plant will receive new supplies every week, along with the personnel coming on and getting off the platform. In addition to food and other essentials for the crew, a supply ship will bring any required maintenance equipment, and other minor requirements. In our current design, personnel will transfer to the hull via docking platforms near the waterline on both sides of the hull and ladders leading to the weather deck, while materiel will be lifted to the weather deck by crane. For significantly larger maintenance tasks, the platform may have to be towed back to a shipyard for longer maintenance periods. It is possible that in further iterations of the design the supplies and personnel may be lifted by cargo lifts outside the hull, or moved entirely by helicopter, if those prove more effective and less expensive. In transferring materials to the OFNP it will be essential to ensure that they contain no contraband materials, and that their integrity has been assured since leaving the terrestrial departure point.

Refueling is another important consideration, the strategy for which has not been entirely yet established. There are a few options for refueling, but the simplest, and the one that will be considered in this paper, will be refueling on site with the spent fuel stored in a pool onboard the platform, sized to accommodate ten or more years of spent fuel, possibly up to the lifetime of the plant. Another major possible option would be the movement of spent fuel rods at some time following withdrawal from the core to a transfer vessel, which will bring them to shore, so that spent fuel need not be stored on the platform beyond the refueling period for its entire life spent. However the option of removing fuel directly from the core to a transfer vessel is likely not practical due to the high radiation field. In any case, ultimate storage of the spent fuel rests with the operator, and a storage site must exist that is not on board the platform unless a national spent fuel repository exists to which spent fuel can be immediately directed upon landing. If there are sufficient OFNPs, the vendor could also create a needed onshore spent fuel site for fuel from multiple platforms.

The refueling outage and significant maintenance activities will involve the transport and residence for various periods of a number of workers significantly larger than those normally on the platform. Security protocols for their entry processing at the Shore Support Facility and chain of custody as they are taken to the offshore platform will need to be defined.

6 Siting and Security Layers

Both careful siting and designation of security layers contribute significantly to the security plan as described next.

6.1 Siting

The OFNP will be sited within territorial waters, as illustrated in Figure 4. The figure also demonstrates California shipping restrictions, which shows that restrictions can be imposed upon shipping, even outside of territorial waters. The plant will be sited at a distance from ports and major shipping lanes and shipping restrictions around the plant will be introduced to increase the time that a threat can be identified and dealt with before approaching the platform.

6.2 Security Layers

The physical layers of the security plan which have been adopted at this time are outlined below. The layers which have

TABLE 6. SECURITY PLAN LAYERS

Layers	Area Definition	Time to Reaction	Time to Breach the Security Layer	Delay	Stop	Eliminate
1) Detection and Assessment	Monitored Area and Controlled Area	Seconds	N/A			
	Large Ship Exclusion Area	Seconds	Half hour			
2) Physical Barriers	Protected Area	N/A	Seconds to Minutes	X		
3) Reactor Layout	Vital Area	N/A	Minutes	X		
4) Plant Security Forces (Onboard and from Shore Facility)	N/A	Minutes	Minutes to a half-hour	X	X	X
5) External Response Forces	N/A	Half-hour	N/A		X	X

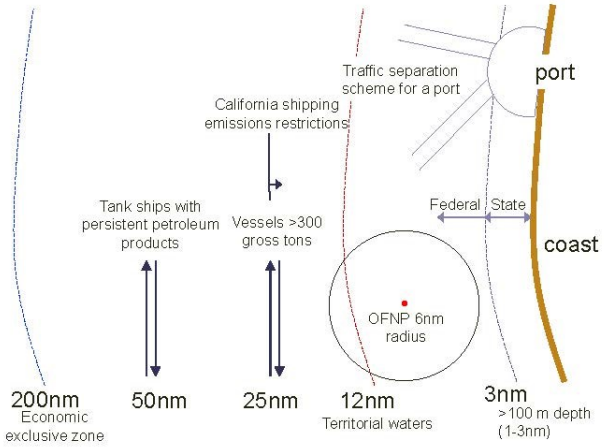

FIGURE 4. OFNP SECURITY ZONES COMPARED TO WATER RESTRICTION AND JURISDICTION ZONES WITH CALIFORNIA AS A REFERENCE CASE

certain defining qualities as outlined in Table 6 are laid out as illustrated in Figure 5. All of these measures are purely qualitative, as a quantitative requirement will be plant-specific and must be determined during the design of each individual plant. The two relevant time qualities are time to reaction - the time it will take for the layer to become operational and ready to meet an attack with full strength; and time to bypass - the time it will take for an attacker to get past the layer and reach the next portion of the reactor defense. Table 4 provides a qualitative estimate for both of these times. While the security forces are to entirely stop the attacker if possible, their objective is to delay them long enough for response forces to arrive if necessary. The response forces goals will be to prevent significant core damage and spent fuel sabotage, and, if that force has already entered the reactor itself, to be able to retake captured plant areas.

The first layer of the security plan will be the detection and assessment layer composed of the Monitored and Controlled Access Areas as well as the Large Ship Exclusion Area. This layer will consist of various detection devices, including radar, sonar CCTV/ Thermal cameras and visual means of detection. The detection devices will have an effective range of detection of several nautical miles, in order to create an effective picture of the surrounding waters a Monitored Area extending about 8 nm from the plant. However, the most important area to be kept under effective observation will be the Controlled Access Area, a 360 degree area of about 1000 meters around the plant, through which maritime traffic is not cleared to enter. Anything detected within that area will be contacted and told to veer off, and the security forces will be brought to an alert status.

In order to protect from the possibility of collision with very large vessels, such as tankers or freighters, a Large Ship Exclusion Area is also specified. This would exclude large vessels of a certain tonnage from a radius of at least 6 nautical miles from the plant such that a large tanker heading towards the OFNP at 12 knots would require 30 minutes to reach the plant. Trespassing of a large ship into this zone would trigger prompt intervention by the host nation coast guard or military forces. The exact tonnage defining such a large ship categorization has yet to be determined, although it will be based on sustainable damage from collision or blast from a large tonnage ship.

The second layer of the plants security plan will be a Protected Area containing multiple physical barriers. These barriers, consisting of booms suspended between buoys, and submarine netting extending underneath the surface, surrounding the plant. The diameter of this protected area will be determined by a blast analysis using the characteristics of the design basis threat and the inherent robustness of the platform design. This Protected

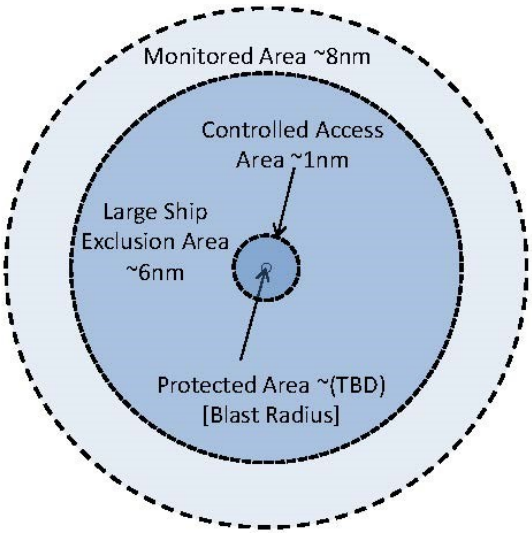

FIGURE 5. SECURITY PLAN LAYERS

Area will have only one approved ingress point, and will serve as a delay to any attacking force. The barriers will give the security force reaction team additional time to respond and slow down attacking ships to make them better targets. In addition, the physical barriers should force explosives-laden ships to detonate at a stand-off range beyond the hull, giving the plant a greater likelihood of survival.

The third layer of the layered defense will be the layout of the platform itself. It will be built with the intention to make it difficult for attackers to be able to board the plant or lethally damage the plant from an off platform location. The exterior hull of the plant will have 12 or 34 meters freeboard above the waterline, and should be thick enough for the reactor to withstand a blast from a medium size boat loaded with explosives detonating at the outer boundary of the Protected Area. There should be firing positions on top of the plants hull, with firing ports and cover for the security force to use.

The fourth layer located on the reactor plant itself - will be the security force itself. Some members of the security force will be on duty at all times, patrolling the top of the plant and looking out for threats. The remaining on-board personnel will make up a quick reaction force, able to respond to a threat within minutes. Their goal is to stop an enemy force if possible, and if not, then to delay the attacker until a response force from military or law enforcement can arrive and destroy the attacking forces. The security forces will be armed with both small arms and some heavy weaponry, to be able to defend against a small boat attack. Others will be trained to operate radar controlled automatic weapons for use against specified targets.

Finally, the fifth layer the plant response force based well beyond the Monitored Area will consist of plant security forces from the Secure Shore Support Facility eight (8) to ten (10) Nautical Miles most likely backed-up by local law enforcement or military forces, available to respond to a threat to the OFNP. The chief of security for the plant will coordinate with this external response force beforehand, to create a contingency plan in the case of an attack. The external response force should be able to arrive on site within a half hour with sufficient force to destroy an attacker and retake the plant if necessary.

7 Key Solution Approaches

In the plant design the nuclear reactor vessel will be placed in a containment structure housed underwater within a hull projecting from the bottom of the plant. The fuel sits behind four steel barriers-the reactor pressure vessel, containment, reactor hull and platform hull. Vulnerable systems sited above the surface of the water include the turbines, turbine/condenser system and some operational support systems while the primary operational and all safety-required systems will be wholly contained in the containment structure under the surface. This forces an attacker intending to disrupt these structures to either adopt an underwater approach, using divers or subs, or launch an attack through the deck of the plant, then entering the containment structure from above. Thus, focus must be placed on designing detection measures, physical barriers and the protection of access points to the deck of the plant itself.

7.1 Strategy for Resisting Attack

The security forces must be capable of countering the security threats identified in Table 1. For meeting these security requirements the platform would be equipped with Fighting Positions (FP) strategically positioned around the plant in order to repel an attack by small boat and subsurface attackers. These fighting positions would be outfitted with both lethal and non-lethal weapons to first warn and deter a potential threat and then stop the threat.

The physical construction of the reactor must be resistant to explosions as well, and able to withstand or redirect the explosive blast of a number of improvised explosive devices at once. The reactor must be able to resist an explosion from outside the controlled zone or farther out from the plant from a medium sized ship loaded with explosives. The reactor must rely on its security personnel to prevent explosives-laden vessels from approaching too closely, but an explosion at a further stand-off range must be considered as well.

To protect the reactor from capture, security personnel must be able to delay a Design Basis Threat force to allow response forces to arrive. The actual time for a response may vary, depending on the location of the reactor, but a half hour should be the upper allowed limit for a response from military and law enforcement. Although physical barriers such as submarine netting

and floating booms will create some delay, the most important factor in the defense of the reactor will be to use security personnel to prevent attackers from penetrating the interior of the reactor structure long enough for a response force to arrive.

Part of the reason conventional, land-based plants possess such large security forces is the necessity of maintaining many constantly manned posts in order to prepare for an attack. The longer the time between the first detection and assessment of a potential attacker and the point at which they reach the platform, the lower the number of constantly manned posts necessary for successful security of the offshore plant. The semi-monthly personnel rotation schedule of the plant means that the security personnel who are not on watch will nonetheless still be on the platform. Those members of the security force who are not at their post at any given time will thus still be able to respond and hence must retain their fitness for duty status at all times while at the plant. When an alert is given, they will have time to prepare for the attack, even if they are not at their post at the time. Therefore, another way to reduce personnel requirements, and thus costs, will be to increase the time between detection, assessment and contact, both by increased detection ranges and by delaying tactics which slow down a potential attacker.

7.2 Security Force Composition

The security force has two components. The first component is the primary security team, consisting of armed officers patrolling the deck and the shore site. The primary security team would have the responsibility for security of the reactor, security of the shore facility, and processing plant personnel transiting to and from the plant at the secure shore support facility. The second component is the technical security team, who man the Central Alarm Station (CAS) and Secondary Alarm Station (SAS) and monitor detection equipment. The technical security team has responsibility for monitoring and maintenance of detection equipment including sonar, radar, CCTV and UAV systems. The number of security force members on the platform at any time depends on two factors the number of security force members needed on watch at any given time, and how often they are expected to stand watch.

The primary on-watch team is intended to provide back-up visual detection to the detection equipment, and to provide initial response actions to an intrusion before the reaction force (consisting of all other members of the security team on the platform) arrives in response to a threat.. Therefore, the minimum security force on watch for the primary security team on the platform will be based on the amount of deck area they are expected to cover visually, and the initial response actions required. It is anticipated that deck area coverage will be the controlling factor for establishment of the watch numbers.

The technical on-watch team is intended to monitor the detection equipment to provide initial warning of an intrusion. NRC regulations require a minimum of two officers in both the CAS and SAS. Although NRC guidelines will not necessarily be binding on an OFNP sited in another country, they nonetheless offer a useful illustration of possible required number of personnel.. The minimum of two anticipates one operator manning the Intrusion Detection System (IDS), which would include radar, sonar and other detection measures, while the second monitors other systems not included in IDS as well as related duties such as access control into restricted and vital areas. Since many of these related duties will be significantly simplified in the OFNP, because access to restricted and vital areas involves entering concentric circles rather than individual buildings, it may be reasonable to only require one officer in the CAS.

The second factor in total numbers of security personnel is the number of off-watch personnel needed to support any given amount of on-watch personnel. The on watch personnel only stand watch for some pre-specified part of the day, which means replacements are necessary for them. If we split the security force into teams of the minimum on-watch security personnel discussed above, then there must be a number of teams sufficient to have meet the watch schedule while allowing sufficient rest and down-time to ensure adequate attentiveness. In addition, extra personnel should be present to provide sufficient allowance for emergencies, medical casualties and other extraordinary events.

Security at the shore site for the plant will be easier to ensure than for a land-based plant. First of all, the cycle schedule for plant workers, who live on the platform for weeks at a time, will reduce the number of personnel moving into and out of security-protected areas each day. Instead, there will be well-anticipated large personnel movements every few weeks, during which security requirements will be higher. Secondly, the shore site contains no Vital Areas or high risk areas, and therefore can utilize a lower level of security requirements than either the platform or an equivalent land-based facility. Thirdly, the shore sites perimeter will be much shorter than that of a land-based plant, also reducing personnel requirements. The shore sites security requirements will be based primarily on normal physical security for warehouses or other less well protected sites, and consists merely of sufficient officers to notice and deter intruders.

An example security force for the OFNP-300 would be 40 officers in total. In this example force, cross-trained primary security force officers operate the CAS on board the plant instead of dedicated technical operators. The members of the primary security team totaling 30 officers would alternate duty on the plant and at the shore facility, spending 2-3 weeks at each. Of these 20 officers will be at the plant at all times. The remaining 10 officers of the primary security team would be acting as security of the shore facility, training or leave. The technical team of 10 officers, based at the shore facility to reduce the costs of basing more personnel offshore, monitors the sensors and detection devices at the SAS and performs preventative and corrective maintenance

TABLE 7. COMPOSITION AND ROLES OF OFFICERS OF THE EXAMPLE SECURITY FORCE

Role	Responders on Plant Site	Responders at Shore Site	Total Force
Primary Security	20 (2 officer team on patrol duty each 8 hour shift, 2 officer team on duty at the Primary Alarm Station each 8 hour shift, 5 teams)	10 (2 officer team on patrol duty each 8 hour shift, 5 teams)	30
Technical Specialists	0	10 (2 officer team on duty at the Secondary Alarm Station each 8 hour shift, 5 teams)	10

on SAS and CAS equipment.

Two of the primary security team would be on watch each eight hour shift each patrolling a 180 degree perimeter section of the plant. At the same time, two more would be on watch each eight hour shift in the Central Alarm Station, monitoring the detection devices, thus also reducing costs by reducing the number of personnel necessary on the offshore platform.

The members of the security team based at the plant would live onboard the plant, ensuring that the plant has a sixteen-man rapid reaction force available at all times. With the use of effective remote sensing devices, the security team would have sufficient warning for timely response by all the onboard security personnel. Table 7 identifies the composition and roles of officers of this example security force for the OFNP-300.

The Security Force enhancement necessary for the larger OFNP-1100 would require about double the complement of the OFNP-300. This is predicated on scaling the size of the Primary Security officer complement by the perimeter ratio of these two sized plants which is 75m/45m= 1.67 or rounded to 2. For the Primary Security officers at the shore site who primarily process workers and materials transiting between the shore site and the offshore platform, scale by plant power rating which is 1100 / 300=3.7 or reduced to 3.5. Hence the resulting number of example Primary Security officers becomes 40 on the plant site and 35 at the shore site. The number of technical specialists remains at 10 yielding a total example force of about 85 officers for the OFNP-1100 based on the example for the OFNP-300 developed above

7.3 Security Equipment

There are three types of equipment which could be utilized by the OFNP security force: detection equipment, to monitor the area around the plant to detect and identify potential hostiles; physical barriers and defenses, which are included to delay attackers and reduce damage in case of explosive detonation; and finally, weapons, both lethal and non-lethal, intended to, first, deter an attacker from approaching, and second, to fend off or eliminate the threat.

The minimum criterion for the detection system is the necessity to detect a potentially hostile activity with sufficient time for the reaction force on board the platform to come on deck to protect the plant. In addition, the detection system should have sufficient range to ensure that the time from identifying a hostile to the response team from a naval base or other military/coast guard installation is minimized. Different potential hostiles will have different approach speeds and different ranges at which they can be detected and identified by the platform detection system, so the detection equipment should be based on the limiting case, which could be either drones or submarines Due to the circumstances of a land-based plant, hostile detection can for the most part only take place on land owned by the plant, using such measures as Closed Circuit TV (CCTV) and thermal cameras and motion sensors to monitor the perimeter of the plant. By contrast, an offshore plant has 360 degree of vision, and can monitor areas far out from the plant.

The following describes an example case of a detection system. The example plant will be equipped to detect vessels up to 24 nautical miles (by radar), detect and assess small craft up to 8 nautical miles (by radar and long range CCTV and thermal camera system) and divers to 3 nautical miles from the plant (by sonar buoys). The radar would be equipped with Automatic Identification System (AIS) to be able to identify commercial shipping traffic within the 24 nautical mile range. This detection range of 8 to 24 nautical miles will allow a full 12 to 36 minutes from detection to arrival at the physical barrier (the boundary of the Protected Area) to which is added multiple minutes of delay needed for the attacking force to breach the physical barrier, which we tentatively estimate as 18-30 minutes as discussed below. Thus the total time for the attacking force to reach the plant from initial detection is 30 to slightly over an hour for a vessel travelling at 40 knots directly at the plant. In that time, the external response force from both the shore facility and host country military and law enforcement will be able to respond if called upon. For the slower vessels that we anticipate as more likely, the time is increased significantly.

The plant will also have eight (8) passive acoustic buoys floating approximately 1.5 nautical miles from the plant. The passive acoustic buoys will have a passive sonar system with the ability to detect a small submersible or a diver at a range of approximately 1.5 nautical miles. The passive sonar-buoys have a lifetime of several years, with a requirement for maintenance

about every three months. Eight (8) passive sonar-buoys would provide overlapping coverage of the area around the plant out to 3 nautical miles even when one sonar-buoy undergoes maintenance. In practice, the machinery noise of the platform limits the interior detection to approximately 0.5 nm from the plant.

If active sonar is used, four (4) active sonar buoys could be located approximately 0.5 nm from the OFNP. At the current time the maximum range for the active sonar to pick up divers is between 600m to 1000m (0.32 to 0.54 nm). Therefore, the sonar buoys will be able to detect divers between about 0.2 and 0.8 nm from the plant at the least, and 0 to 1 nm if conditions are favorable.

Automated analysis of sonar data may further reduce personnel costs, since the plant Central Alarm Station (CAS) will not require dedicated sonar technicians to detect contacts. Of course, the security personnel in the CAS will still monitor the raw sonar data as a backup to the automated detection system, but there will not be a need for a separate sonar technician. An algorithm for automatic flagging of sonar contacts which will fit the requirements of the offshore platform very well has recently been developed [11].

In addition to electronic detection means such as sonar and radar, the plant will also use unmanned vehicles for detection and identification of contacts. The unmanned vehicles will help with redundancy in detection means. More importantly, however, they will be able to identify a potential threat and therefore determine appropriate responses earlier. They will be able to approach an alarming contact and determine whether the contact is a threat that must be responded to with lethal force, non-lethal force, or merely warned away. The unmanned vehicles may be airborne vehicles, but water unmanned vehicles will be less costly and equally effective for the purposes required. Using unmanned vessels for the purpose of re-directing or deflecting an incoming vessel from its course, or an airborne attack by a small aircraft or drone, is also contemplated, and may help decrease the threat of air attack or collision.

In order to further delay a threat and allow the security force time to respond, physical barriers around the plant will delay a potential attacker to allow an effective response. These barriers will take two formsbooms from and around the plant defining the perimeter of the Protected Area and the design of the plant itself. The criteria for the outer layer of booms is to stop a medium-sized ship at a sufficient distance that an explosion would do negligible structural damage to the plant. Effective layout of the plant, such as ingress points and the placement of the ladder ways into the interior of the plant, will serve to delay attackers as much as possible, and the plant itself will be hardened against explosions, as mentioned above, to prevent containment breaches or damage to the integrity of the plant if an explosion or collision is used by an attacker to try to damage the plant. The criteria for the plant design is to withstand a collision of a large ship and an explosion from a small boat alongside the plant. Equipment to move the plant out of the way of a collision or explosion, such as specially designed mooring lines or dynamic positioning units, will also be considered in the future.

In an example case, the physical floating barrier around the plant, having a 3 m elevation above the water and holding netting below them which will wrap around the underside of the plant, serve the main purpose of delaying both small, fast boats and larger craft. The physical barrier is intended to delay an attacker for the maximum time possible, and we will confirm the estimated delay time of between 18 and 30 minutes when more specific barrier design characteristics can be established. This delay of any attacking craft will give the security forces on board the platform time to respond.

Finally, the OFNP will require systems to actively deter, stand-off and potentially destroy attackers. This includes both lethal and non-lethal weapons as well as warning systems. The criteria for the non-lethal and warning systems will be the ability to reach a potential aggressor in the Controlled Access Area and deter them from approaching closer. These systems are intended to differentiate between active hostile intent and non-lethal intent such as demonstrators. The lethal weapons systems (currently under NRC Section 161A Authorized Weapons, the largest approved weapon is the 50 caliber machine gun) would be able to destroy small boats of up to approximately 20 feet and damage and redirect larger vessels. In addition, there must be sufficient small arms to engage multiple teams of attackers.

There are a number of non-lethal systems available which can first warn approaching vessels or aircraft/drones of their entry into our Controlled Air Space/Access Area and then can be employed as a further deterrent to their continued penetration into this Area towards the plant platform. These systems include a Long Range Acoustic Device (LRAD) for acoustic hailing and as a sonic weapon, a Long Range (3/4 mi) LASER that can dazzle the crew of an approaching vessel so they are unable to aim weapons, the USNAVYs Long Range Ocular Interrupter (LROI) a bright beam of visible light with varying intensity for which low is for visual warning and high for temporary visual suppression and an Active Denial System (ADS) which shoots beams of millimeter waves which heat up the intruder within three (3) seconds which highly motivates escape behavior (the Raytheon Silent Guardian uses this type of technology). The LRAD system is offered within an integrated Radar, Thermal and CCTV system by the ECSIs Anti-Piracy solution package. In addition to deterrence, disabling the propulsion or steering of an approaching vessel may be an attractive way to reduce their effectiveness as well as fend off non-lethal attackers. Unmanned vehicles could allow targeted attacks on steering or propellers, and potentially boarding an approaching vessel could be an option as well.

Potential lethal weapons packages include 9mm hand gun, semi- automatic assault rifles, short and long barrel 12 gauge shot guns, .30 caliber rifle and enhanced weapons such as standard radar controlled .50 caliber machine guns.

8 Costs

Security is a large cost in modern reactors, due to increased requirements since 9/11. The three major cost-factors for the security of the OFNP will be personnel, hardware and maintenance, in that order. At this stage of our design personnel costs will be the highest contributor to security cost, as is true for security on land-based plants. Unfortunately, personnel costs per person will rise for an offshore plant, due to both the cost increase for a member of the platform security force compared to a land-based plant member and also partly due to the transportation costs associated with getting him and his sustenance to the platform and back again. This means that personnel costs will be the highest expense of the security plan, unless the personnel requirement can be sufficiently reduced.

The annual salary of an offshore platform nuclear security officer can be estimated, based on the salary of a conventional nuclear security officer and the salary of an oil platform worker. The annual salary of a nuclear security officer ranges from around $50,000 to $70,000. By contrast, the annual salary of an oil platform worker is closer to $100,000. We will assume that the annual salary of the security personnel for the plant will be approximately $100,000, like an oil rig operator. In the example developed above, the OFNP-300 plant will have a total of approximately 40 security personnel, which means that the personnel cost for the security personnel will be $4 million/year.

Hardware costs will also be a cost-driver, although they will contribute less than personnel costs. Unlike personnel costs, the hardware costs for the OFNP-1100 version should not increase appreciably with the larger platform. Required small arms will increase proportionally with security force numbers, but the increase in size will not necessitate more purchases of sonar buoys or radar systems. There will be a greater requirement for physical barriers, but the increase should not be significant. The estimated costs for each are shown in Table 8.

Hardware costs include both the one-time costs of purchasing equipment such as weapons and detection equipment (shown in Table 8 as $1.685 million if passive sonar is used) and the security monitoring equipment of $1.65 Million. This totals to a security cost of $3.335 Million, lower than the yearly recurring personnel cost of $4 million/year.

Finally, maintenance costs are harder to account for, but to a large extent, they can be folded into the total maintenance costs of the platform. The main maintenance intensive pieces of hardware will be the alarm stations and their command and control equipment, and the sonar-buoys and radar systems. Since the maintenance labor is accounted for in the technical security force, then a workable, conservative rule of thumb is to use 15% of initial equipment costs as an annual equipment repair/or replacement estimate. Factors such as warranty and obsolescence which are cost contributors over the 60 year life cycle of the plant are included in this estimate. Hence we estimate the maintenance cost for those pieces of equipment as approximately $530,000/year. Thus, rounding slightly, the overall cost of the security for the OFNP-300 will total a one-time hardware cost of $3.3 million, with a further annual personnel and maintenance cost of $4.5 million. This gives an annual cost of 0.155/kWh for the OFNP-300, a 300 MWe reactor operating at a 90% capacity factor. The one-time cost, normalized to plant life, will be about 0.013/kWh, assuming a 10 year equipment lifetime. Comparatively, the annual security cost for the three pressurized water reactor units operated by Xcel Energy in Minnesota in 2010 was $25.5 million according to public documents, which do not, however, provide a breakdown of cost elements [12]. The three units were rated 585 MWe (since up-rated to 670MWe), 550 MWe and 550 MWe respectively, totaling 1.7 GWe. This gives an annual cost of 0.192 cents/kWh for security of the Xcel reactors, a value close to the estimate above for the OFNP-300. Based on the estimates above, the OFNP-1100 security costs will only increase by a factor of two or less, while the electricity output is more than tripled. Thus, the security cost per MWe for the OFNP-1100 will be significantly lower than that for other plants of comparable size, at least according to easily available cost data and the rough scaling factor expressed in the previous section.

TABLE 8. ESTIMATED COSTS OF SECURITY EQUIPMENT

Equipment	Cost ($1000s)
Weapons and Detection Equipment:	Total: 1685 (passive sonar) or 2715 (active sonar)
CCTV and Thermal Cameras	35
Radar (with AIS)	250
Passive Sonar Buoys + Control	610
Active Sonar Buoys + Control	1640
Unmanned Vehicles	assume 100 (for four units)
Physical Barriers	600
Non-lethal Weapons (LRAD, LOI, ADS)	50
Lethal Weapons	40 for 30 man force
Security Monitoring Equipment:	Total: 1650
CAS and SAS	500
Plant Internal Spaces	150
Shore Site	1000

9 Future Work

Significantly more work will be needed to further detail the security of the OFNP. Firstly, work must be done on less well studied threats, including underwater threats, possible attacks from drones or unmanned vehicles, and the possibility of collision. Work is currently in process using industry knowledge and collision modeling software to assess the collision threat and possible responses or mitigation, such as using mooring lines or dynamic positioning units to move the platform out of the way of a collision. Initial analysis has also been done on the underwater threat, tentatively investigating possibilities including the use of torpedoes to destroy incoming threats, unmanned underwater vehicles and physical barriers such as netting. However, more work will still help clarify useful responses and their costs.

Secondly, the security plan needs to be expanded to include non-standard conditions, particularly refueling and other major maintenance operations which necessitate larger and less standardized personnel movements. These will be developed in parallel with iterations in the operational strategy for refueling and major maintenance operations. Such situations should mainly involve dealing with an increased number of personnel, and therefore will be only quantitatively, not qualitatively, different from normal operations.

Thirdly, the threat environment and government support should be analyzed in different potential platform sites. For example basing the platform off the coast of the United States will impose different security requirements than basing it off Singapore, due to different potential threats, different levels of government support and potentially different regulatory environments. When operating an actual OFNP these differences will need to be taken into account, and although the specific conditions may not be definable with accuracy now, work can be done on estimating the differences that may occur in different conditions. Finally, work must be done to further specify the exact personnel and equipment requirements through further iteration of design and requirements. Requirements may be reduced through adoption of additional hardware solutions or from further analysis of the security conditions.

10 Conclusions

The most difficult security scenario to deal with is a scenario in which the attackers are trying to damage the plant, not capture it. In particular, an offshore plant faces the relatively unique vulnerability compared to a land-based plant that it can be sunk, whether by an explosion, a ship collision, or both. Further examination and analysis is needed to determine the best responses to an attack by a suicide bombing attack, remote control drone attack, or an intentional ship collision, but the major concepts of the response are captured here delay of the attacking force and protection of the containment.

The initial estimate in this paper of security cost for the OFNP-300 of 0.155 cents/kWh for the offshore plant is slightly lower than that for a 3 unit PWR land based station for which costs have been reported publicly and quoted in this paper. Due to security concerns, however, publicly available information does not include numbers of security personnel or other, more detailed information. Land based Nuclear Power Stations have not addressed air attack by drones and nor yet have we but may further investigate the subject in the future.

Cost-savings are mainly accessible if compensatory means can be designed to achieve reduction in the security force required for the plant since as confirmed in Section VII, the one-time hardware costs are relatively minimal. They amount to less than one year of security annual expenditures, and thus are very small compared to the personnel costs. Ideally, a further personnel reduction could be occasioned by larger hardware spending.

Finally we stress that the security plan we have presented is merely an example of how the assumed design requirements might be responded to. Further consideration is required before we will have reached the stage of sufficient understanding of the security threats as well as the most effective licensing framework for this application to be definite in recommending a definitive security plan for the OFNP. In this regard an ambitious challenge contemplated for study is the development and exercise of a risk-informed security strategy to replace the deterministically-based current USNRC regulatory structure which has been assumed as the required design basis for the security plan presented in this paper.

Acknowledgements

The suggestions of Richard Rosano, Talisman International for enhancing the clarity and scope of this paper are gratefully acknowledged, as is the assistance of Brian Holian, NRC Division of Security Operations. The assistance of Grant Genzman, MIT graduate student in developing the siting strategy and the security layer arrangement is gratefully acknowledged as well.

REFERENCES

[1] Buongiorno, J., Jurewicz, J., Golay, M., and Todreas, N., 2016. The offshore floating nuclear plant (ofnp) concept. Accepted for publication in Nuclear Technology.

[2] Westinghouse Electric Company, 2014. Ap1000 nuclear power plant.

[3] Memmott, M. J., Harkness, A., and Wyk, J. V., 2012. "Westinghouse small modular reactor nuclear steam supply system design". In Proceedings of the International Congress on Advances in Nuclear Power Plants, pp. 973–983.

[4] Partners, B. ., 1982. *Islands for Offshore Nuclear Power Stations*. Graham & Trotman Limited.

[5] 2b1st Consulting. Spar. http://www.2b1stconsulting.com/spar/.
[6] Noyes, R., ed., 1977. *Offshore and Underground Power Plants*. Noyes Data Corp.
[7] Kaiser, M., Snyder, B., and Pulsipher, A. G., 2013. Offshore drilling industry and rig construction market in the gulf of mexico. Tech. Rep. BOEM 2013-0112, U.S. Department of the Interior.
[8] Minelli, P., Buongiorno, J., Golay, M., and Todreas, N., 2015. "Balance of plant and power transmission for the offshore floating nuclear plant". In The 16th International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH-16).
[9] Jurewicz, J., Buongiorno, J., Todreas, N., and Golay, M., 2014. "Conceptual design of an offshore floating nuclear power plant with spar-type platform". In The 10th International Topical Meeting on Nuclear Thermal Hydraulics, Operation and Safety (NUTHOS-10), Dec. 14-18, 2014, no. Paper 1104.
[10] Jenkins, B. M., 1989. Potential threats to offshore platforms. Tech. rep., RAND Corporation, Santa Monica, California.
[11] DeMarco, K., West, M., and Howard, A. Sonar-based detection and tracking of a diver for underwater human-robot tracking scnearios. Georgia Institute of Technology. To be published.
[12] Koehl, D., 2010. Direct testimony and schedules before the minnesota public utilities commission, state of minnesota, in the matter of the application of northern states power company, a minnesota corporation, for authority to increase rats for electric service in minnesota. Tech. rep., Minnesota Public Utilities Commission.