International Journal of Nuclear Security

Volume 4 | Number 1

6-30-2018

# Recommended Corrective Security Measures to Address the Weaknesses Identified Within the Shapash Nuclear Research Institute

Khadija Moussaid
*University of Ibn Tofail*

Oum Keltoum Hakam
*University of Ibn Tofail*

*International Journal of Nuclear Security, Vol.4, No.1, 2018*

# Recommended Corrective Security Measures to Address the Weaknesses Identified Within the Shapash Nuclear Research Institute

Khadija Moussaid
MSc student, University of Ibn Tofail, Kenitra, Morocco

Oum Keltoum Hakam
Professor, University of Ibn Tofail, Kenitra, Morocco

## Abstract

The Shapash Nuclear Research Institute (SNRI) data book was issued by the International Atomic Energy Agency (IAEA) in 2013. The hypothetical facility data book describes the hypothetical site, which is divided into two areas: the low-security area, known as the administrative area, and the very high-security area, known as the protected area. The book contains detailed descriptions of each area's safety and security measures, along with figures of multiple buildings in both areas, and also includes information about the site's computer networks.

This paper aims to identify security weaknesses related to the institute's location, the Administrative Area (AA), the Protected Area (PA), and the Instrumentation and Control Technology system (ICT) within the SNRI and proposes corrective actions to improve the site's security measures against malicious acts, based on the IAEA nuclear security series publications, and ultimately proposes a new layout for the whole site and the research reactor building presenting the changes made, using a software called Edraw Max.

## I. Introduction

Nuclear and radioactive materials have been significantly useful for humankind in medicine, agriculture, and industry and for helping states with nuclear power plants to produce electricity and meet the increased demand of energy supply while having a clean source of energy. Although these materials are used for pacific purposes, they could also have devastating consequences should they fall into the hands of criminals and terrorist groups.

The IAEA has issued such a data book, the *Hypothetical Facility Data Book: The Shapash Nuclear Security Research Institute (SNRI)*, to help member states, experts, and researchers study a hypothetical nuclear facility to practice nuclear security measures and as an educational tool in tabletop exercises, workshops, and trainings. The data book describes security measures at different areas of the facility, with the measures containing vulnerabilities for the reader to discover and learn from.

Our research developed out of such a tabletop exercise, for which this article is the result. Our article begins with an overview of the SNRI, describing the administrative area, the protected area, and the

computer network. We then identify the various weaknesses relating to the site's location, the administrative area, the protected area, and the instrumentation and control system (ICT), and we propose corrective measures for each weakness. We conclude by suggesting a new site layout for both the overall facility and the research reactor building.

# II. The Shapash Nuclear Research Institute Site Overview

The Shapash Nuclear Research Institute is a hypothetical research institute. It is the "Republic of Anshar's" first nuclear energy research facility. The facility has two major areas: the administrative area and the protected area (Fig. 1).

**The Administrative Area (AA)** is surrounded by a 2.5-meter-high fence. Personnel entering the site entrance gate must pass through an access control point where they must present badges and be vetted by the guard, who ensures that the badges are valid. The procedure is repeated for off-hour access. The personnel phone the guard in the central alarm station (CAS) from a telephone at the gate; possession of a valid site badge is the only prerequisite for gaining access.

All buildings within the AA are not alarmed—including the radioactive waste site, classified as category III. The waste site is used for the storage of radioactive waste from various buildings, such as the research reactor and the fuel fabrication building. The site is under 24-hour surveillance by guards on foot patrol.

The security officer verifies the decals and badges of vehicles entering the site before allowing access. A delivery vehicle must present shipping documents to be verified and ensure that the vehicle has a delivery for the institute, and after a check, the guard makes sure that the recipient is expecting a delivery; if correct, the vehicle is searched for contraband. Personnel and vehicles exiting the site are not checked in any way.

**The Protected Area (PA)**: The very high-security area contains the research reactor building, the fuel fabrication building, support buildings, the oxide storage bunker, the road and rail transportation terminus, the main cafeteria, and the shipping and receiving building. The area is surrounded by two 2.5-meter-high chain-link fences 5 meters apart, with guards towers located at each corner within the protected area perimeter. Patrols of the perimeter are carried out by a foot patrol guard on the patrol road on a random basis.

To access the PA, personnel must pass through metal and radiation detectors in a contraband search. Items in possession are X-rayed, passing through metal detectors. If an individual fails the metal detector search, the procedure is repeated. Personnel exiting the PA pass through a radiation portal monitor, and if no alarm sounds, they continue through the exit door.

A guard verifies vehicles to ensure that the drivers have badges allowing access to the institute, before a gate permits entry. The guard checks the vehicle for contraband, and once the inspection is complete, the gate is unlocked, permitting entry of the vehicle to the SNRI-protected area.

**The computer network** of the facility operates under a system that connects a number of computer systems, forming a local area network with protocols which control the passing of information.

The research reactor, the fuel fabrication area, and the central alarm station contain sensitive information and, thus, operate on a *red* network. The server for the administrative network (the *yellow* network), which contains all administrative functions, is located in the administration building. Information on the *green* network, also called the general network, is available to the general public.

The plant's own telecommunication system is used to provide analog and digital connections, but the unavailability of analog spares forces the site to change to digital ICT. Data threats that the SNRI has

experienced include hacking attempts, reported by the computer network engineering group, and intercepted communications from a neighboring country **[*1*]**.

# III. Identification of the SNRI Security Measures' Weaknesses and Proposed Corrective Actions

In examining the SNRI site, we identified weaknesses relating to the location of the institute, the administrative area, the protected area at the level of the fuel fabrication building, the research reactor building, the Nuclear Material Accounting and Control (NMAC) organization, contraband detection equipment, and the shipping and receiving building and the instrumentation and control system ICT. In the tables below, we discuss these weaknesses and propose corrective actions which, we believe, can improve access control procedures, the physical protection system of the facility, and information security.

## A. Location

| Weaknesses | Proposed corrective actions |
|---|---|
| 1. • The institute is located in the country's capital, which presents crossroads of trading lanes;<br>• The city's inhabitants live in poor conditions and resent the institute. | 1. • Siting a nuclear facility in a busy city increases the probability of malicious acts attempts. A suitable site for a nuclear facility should be selected prior to designing the facility, taking into consideration population distribution and other factors that could comprise security measures. States with an interest in the development of nuclear power projects should also take into consideration multiple criteria for which consequences of a potential accident would be at acceptable limits:<br>- The costs are minimized.<br>- The site characteristics (population distribution, meteorology, hydrology, etc.).<br>- Low probability of phenomena occurring **[*2*]**. |

## B. Administrative Area

| Weaknesses | Proposed corrective actions |
|---|---|
| 1. The site entrance gate is unlocked and open during normal working hours; intrusion could occur when guards are absent. | 1. The site entrance gate should be locked and alarmed to prevent and detect any unauthorized access and to complete the security personnel job. |
| 2. Possession of a valid site badge is the only requirement for off-hours access, which could increase unauthorized access. | 2. • Technical means and procedures for access control to authenticate an individual's identity to confirm that the name and the personnel particulars of the individual in question are correct **[*3*]**.<br>• For off-hours access, personnel should have an authorized slip listing their requisite task, the area where the task is to be carried out, and the amount of time needed. Security personnel then compare the slip's information with the information he/she has been informed of in |

| | |
|---|---|
| | advance; if the information matches, the personnel are escorted to their designated posts. |
| 3. Administrative area buildings are not alarmed, which could assist adversaries in achieving malicious acts. | 3. Buildings within the AA should be alarmed so as to detect any intrusion. |
| 4. The radioactive waste site is located within the AA, a low-security area; unauthorized removal of nuclear material can be carried out by an insider. | 4. The radioactivity waste site shouldn't be located within the AA, but rather, in a higher-security area. |
| 5. Vehicles and personnel exiting the AA are not checked, making it easy for an insider to leave the premises with unauthorized materials or having committed malicious acts. | 5. • Vehicles, persons, and packages entering and exiting the AA should be subject to search for detection and prevention of unauthorized access.<br>• Parking area should be located farther from both the administrative and protected areas to prevent unauthorized access to them. |
| 6. Most senior management personnel have keys to the outer doors of the administrative buildings, and access to multiple zones within the site increases the chance of an insider carrying out a malicious act. | 6. All employees should only have keys to his/her personnel post; even senior management personnel could conceivably have malicious intentions. |

## C. Protected Area

| **Weaknesses** | **Proposed corrective actions** |
|---|---|
| 1. Fences surrounding the protected area are only 2.5 meters high. | 1. The protected area should be ringed by two parallel fences of a 3-meter (minimum) height and topped with strands of barbed wire, the inner fence providing a physical barrier to prevent unauthorized access and supplemented by intrusion detection equipment. The outer fence reduces false alarms triggered by people or animals **[*4*]**. |
| 2. Patrol inside the perimeter of the protected area is conducted by only one guard on foot, which is not extensive enough for such a sensitive area. | 2. Guards should patrol the protected area at scheduled hours, but should also patrol the area at unscheduled hours to prevent an adversary's calculations **[*5*]**. |
| 3. Unauthorized access can occur during work hours, since access points are always open throughout the week. | 3. Identity of authorized persons entering the PA should be verified; passes or badges should be issued and visibly displayed inside the PA. |
| 4. The VIP parking area is located inside the protected area. | 4. • The parking area—including VIP parking—should be located far from both the administrative and protected areas.<br>• Portal display monitors should be installed in conjunction with physical protection systems so that portals are properly staffed for surveillance and detection **[*6*]**. |

| | |
|---|---|
| | • To prevent unauthorized vehicles from entering the facility, vehicle barriers should be placed at a suitable distance from the inner area **[*6*]**.<br>• Effective physical protection systems comprise three axes:<br>—Detection: requiring technical means, such as intrusion sensing and access control.<br>—Delay, using barriers, response forces, and distance.<br>—Responses which will be driven by professional security staff and an off-site law enforcement body **[*3*]**.<br>• The central alarm station (CAS) should always be staffed for monitoring and evaluating alarms and should ensure communication throughout the facility with the response guards **[*6*]**.<br>• The central alarm station should be secured in such a way that acquired information won't be lost or altered in the event of a threat.<br>• An uninterruptible power supply should be provided and protected against unauthorized manipulation for the CAS, communication, and alarm equipment **[*6*]**. |
| 5. The cafeteria is located the protected area, which leads to unauthorized personnel regularly entering and exiting the PA. | 5. The cafeteria should not be located within the protected area, so as to minimize unauthorized access to the area. |
| 6. The road and rail transportation terminus is located within the PA, which is neither secure nor safe, even with robust security measures, thus placing the entire site in danger. | 6. Security measures for shipping and receiving materials should be kept to the shipping and receiving building. |

### *1. Fuel Fabrication and Reactor Building*

| **Weaknesses** | **Proposed corrective actions** |
|---|---|
| 1. Oxides stored on open shelves in the fuel fabrication building, as well as experiment materials in room R091 (Fig. 4) in the reactor building, can easily be stolen in the event of unauthorized access. | 1. Material containers placed on open shelves should be caged in order to increase the time required for completing malicious acts. |

| | |
|---|---|
| |  <br>Fig. Caged Material |
| 2. The main entry doors are made of regular glass; an offender could easily break in. | 2. Doors should be made of bullet-resistant glass, not regular glass. |
| 3. There are no alarms in the offices or sensors on the office doors in off-hours, and an intrusion therefore wouldn't be detected. | 3. Tamper indicating devices (TIDs) should be installed on critical cabinets. |
| 4. Information showcased in the foyer in the fuel fabrication building could help an adversary to carry out malicious acts. | 4. Site details shouldn't be displayed, even for visiting dignitaries. |
| 5. There is no metal or nuclear material detector at the emergency exit of fuel fabrication building's administrative area. | 5. Tampering emergency doors should be installed at the reactor and fuel fabrication buildings. |
| 6. Room R091 is next to the personnel emergency exit door; in the event of emergency, unauthorized theft from the room could be carried out by an insider. | 6. Separate the emergency door from the shipping door to avoid material being removed in the event of an emergency. |
| 7. No CCTV cameras are installed at vital areas to record entering and exiting personnel. | 7. • Install CCTV cameras covering the main entrance and the reactor shipping/receiving door. Install an additional CCTV camera to cover the entrance to the fuel fabrication building (Fig. 5).<br>• The live camera should be monitored inside vital areas, with the option of recording.<br>• All individuals requiring access to the reactor hall should be vetted, including students during pedagogical visits from universities—who should submit request forms to the national regulator.<br>• Temporary personnel with access to the facility, such as visitors or construction workers, should be escorted to ensure security **[5]**. |

### *2. NMAC organization*

| **Weaknesses** | **Proposed corrective actions** |
|---|---|
| 1. • A single individual is assigned the responsibility for technical coordination of the overall NMAC programs; the individual could manipulate the system without being detected.<br>• The measurement control coordinator is the only person able to verify the measurement equipment; not applying the two-person rule would make it difficult to detect manipulation.<br>• The two-person rule is not applied to samples of category III, thus increasing the chance of an insider carrying out unauthorized action. | 1. • Apply the "two-person rule," which requires that two qualified individuals work together at the same time and location at all times. This rule provides a high level of security to attractive nuclear material and can serve as a means for detection **[*5*]**.<br>• Account for and control all materials by use of an inventory. Any detected inconsistencies should be reported to the facility manager<br>• Conduct quality assessments of the NMAC system, including normal operation and emergency conditions **[*7*]**.<br>• Apply the graded approach: as consequences increase, a high level of protection is needed **[*8*]**.<br>• Raise awareness about nuclear security culture through trainings and drills.<br>• Conduct a continuous improvement plan process to learn from past incidents. |
| 2. The SNRI has eight (8) Material Balance Areas (MBAs), but all accountable nuclear material is maintained in just one of them. | 2. Keep an inventory of all nuclear material at the SNRI at each MBA, with each having its own Key Measurement Points (KMPs). |

### *3. Contraband detection equipment*

| **Weaknesses** | **Proposed corrective actions** |
|---|---|
| 1. • The health physics personnel make any required adjustments to equipment, as the technical unit does not receive training in nuclear detection equipment; the health physics personnel could manipulate the detection systems for later intrusion.<br>• The head of the health physics department locks the key to the radiation portal monitor control and sensitivity adjustment in a safe in his office; the password to the safe could be guessed by the unauthorized personnel, gaining access to the key. | 1. • Keep records of all personnel with access to or possession of keys or systems that control access to areas where nuclear material exist **[*6*]**.<br>• Train personnel undertaking responsibilities of sensitive positions such as radiation control. |
| 2. If the supervisor code is entered, several basic sensitivity programs can be selected with one keystroke. | 2. Multiple barriers should be in place, which would need to be passed before reaching sensitive programs. |

### *4. Shipping and receiving facility*

| Weaknesses | Proposed corrective actions |
|---|---|
| 1. • Waste packages are transferred to the shipping and receiving facility for later transfer to the radioactive waste site; in the absence of security guards, nuclear material could be removed without being detected.<br>• Oxide powders are often left in the shipping and receiving facility for two to three hours while the receiving paper work is completed; these materials are checked by patrol guards every 30 minutes. Theft of material could occur in the interims. | 1. • Materials left at the shipping and receiving facility while paperwork is finalized should be monitored at all times.<br>• Effective communication between all entities with responsibility of assuring secure transport (guards, response force, shipper, and receiver) should be ensured.<br>• Separate the loading and unloading docks, with security guards at each gate (Fig. 3).<br>• The warehouse manager office should be located at the shipping and receiving facility to monitor operations.<br>• Truckers should be escorted and separated from sensitive materials. |

## D. ICT Operations and Information Security:

| Weaknesses | Proposed corrective actions |
|---|---|
| 1.• The republic of Anshar's nuclear regulator does not yet have a regulation for information and communication technology system; thus, the responsibility falls on the plant operator. Not having such a policy means that responsibilities are not defined, and there is no outline of the current requirements, operations, interdependencies, risk, and control. | 1. • The state should establish a policy for information security under its legislative and regulatory framework. This consists of outlining a definition of information security, roles, and responsibilities of all personnel dealing with sensitive information and risk management plan based on a risk assessment approach conducted by the state.<br>• Conduct periodic evaluation of the procedures to ensure that they stay up-to-date and to remind staff members of the importance of adhering to the organization's policy **[*9*]**.<br>• Ensure that goals set by the organization are regularly compared to results **[*9*]**.<br>• Involve staff members in intellectual and physical activities in order to avoid relying on automation systems, which can put humans in dangerous situations. |
| 2. • The unavailability of analog spares forces the Shapash reactor team to shift toward digital information and communication security systems, and not having enough training during transition from analog to digital would increase the likelihood of intrusion into the site's information system. | 2. • The technical unit should undergo training during the transition from analog to digital systems. |

| | |
|---|---|
| 3. • The cyber security manager and the system administrator are the only personnel with access to all networks, making it difficult to detect any manipulation. | 3. • Apply the "two-person rule" for sensitive positions, such as cyber security management. |
| 4. • The operating group adds and removes users and users' rights on behalf of the responsible party in each section, which would give them the advantage of manipulating information. | 4. • Only approved and qualified users should be allowed to make modifications to the systems **[*10*]**.<br>• Passwords should be changed frequently, and multiple barriers to reaching information should be applied.<br>• Modifications and updates to hardware or software systems should be made based on an administrative procedure. |
| 5. • Electronics engineers should be hired, but because of long-term contracts with present staff, no additional employees can be hired; hence, external skills have to be contacted, which means more unnecessary access to the site. | 5. • Implement a career enhancement policy for all employees within the organization, and evaluate the current positions' importance so as to have more opportunities for hiring personnel with requisite skills.<br>• Prior to employment, potential employees should go through identity and background checks and generic medical and psychological assessments, as well as checks of all declared degrees. |
| 6. • The SNRI have experienced hacking attempts reported by the computer engineering group. | 6. • Ensure confidentiality, integrity, and accessibility so as to protect information from disclosure to unauthorized parties, modification, and denied access **[*10*]**.<br>• The computer security program must include a rapid means of responding to incidents—describing how to maintain the ability to quickly detect and respond to computer attacks, mitigate the consequences of cyber-attacks, correct exploited vulnerabilities, and restore affected systems, networks, and equipment **[*10*]**.<br>• Sensitive data should be backed up in at least three different places.<br>• The classification of computer systems should be taken into consideration when defining the appropriate level of security to be applied.<br>• Improve and enforce strict control over the use of media and portable equipment. In the case of USB drives, CDs, and laptops being used to interface with the facility's hardware, measures should be in place to minimize the threat of cyber-attacks, such as: |

| | |
|---|---|
| | —Minimize the use of devices not maintained at the factory.<br>—Use virus detection devices both before and after being connected to the facility's equipment.<br>—Implement additional security measures for data that comes from sources or devices not a part of the facility.<br>• Conduct security audit checks to help review the facility security risks.<br>• Raise awareness about the importance of maintaining the integrity of information by reinforcing the computer security culture **[*10*]**. |
| 7. • All of the facility's employees have access to the operational documents of the nuclear process in both physical and digital form; such access to sensitive data could facilitate malicious activity from the inside. | 7. • Users should only have access to information necessary for carrying out their individual jobs. |

# IV. Alternative Site Layout:

The changes suggested in the corrective actions above are included in both layouts below.

The areas framed in red are ones modified in the new site layout; areas framed in blue in the new site layout are modifications we've proposed.

**Site Layout:**

- The radioactive waste site is no longer within this area and is replaced by the cafeteria originally located in the protected area; unauthorized personnel won't have access to the protective area, and the waste site will be more protected in the PA, a high-security area.
- The VIP parking area is no longer inside the PA and is separated from both the AA and PA.
- The access control building is located such that personnel and vehicles entering/exiting the site will be inspected.
- Loading and unloading docks are separated at the shipping and receiving building.
- Both the outer and inner fences are 3 meters high.

**The Research Reactor Building:**

- The emergency exit is separated from the shipping door and covered by a CCTV camera. The control room has been added (Fig. 5) with the purpose of controlling material shipped in and out of the research reactor building.
- The nuclear materials placed in room R091 on open shelves are caged; this modification will serve as a delay measure in case of unauthorized access to the building.

*International Journal of Nuclear Security, Vol.4, No.1, 2018*

## The site layout as described in the data book:

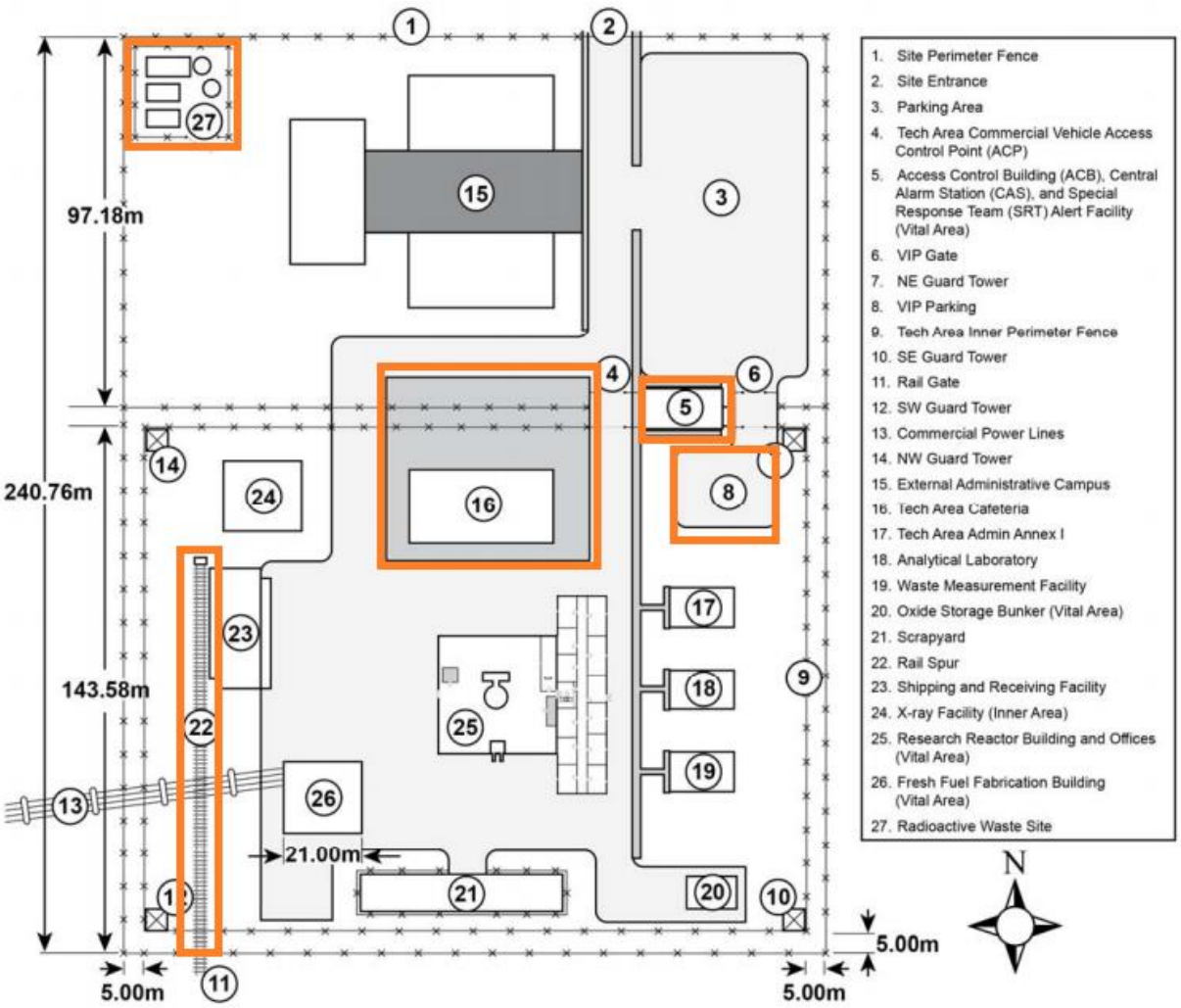


*Figure 1: The Site Layout as Described in the Data Book*

## The new site layout:

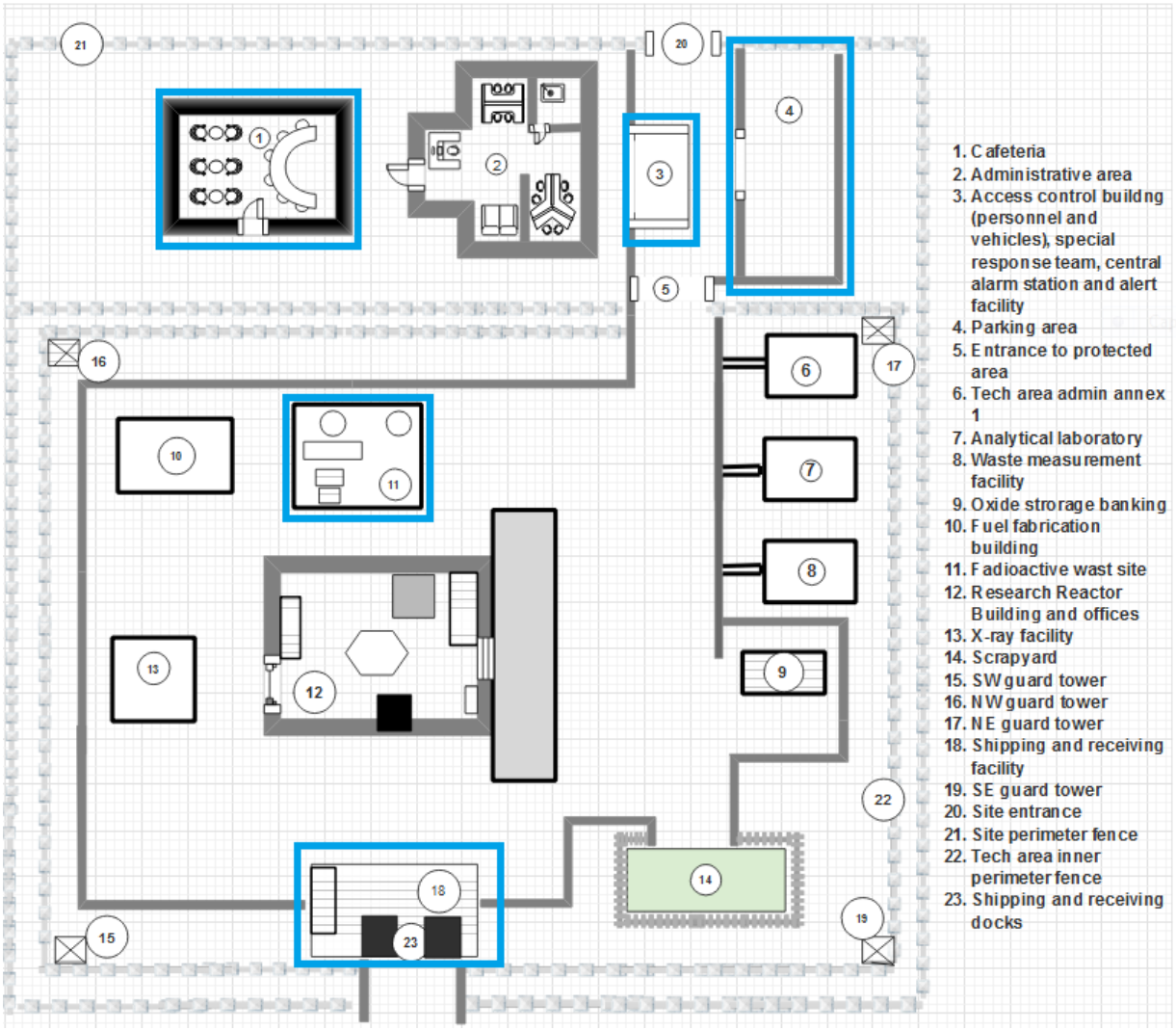


*Figure 2: The New Site Layout*

**The research reactor as described in the data book:**

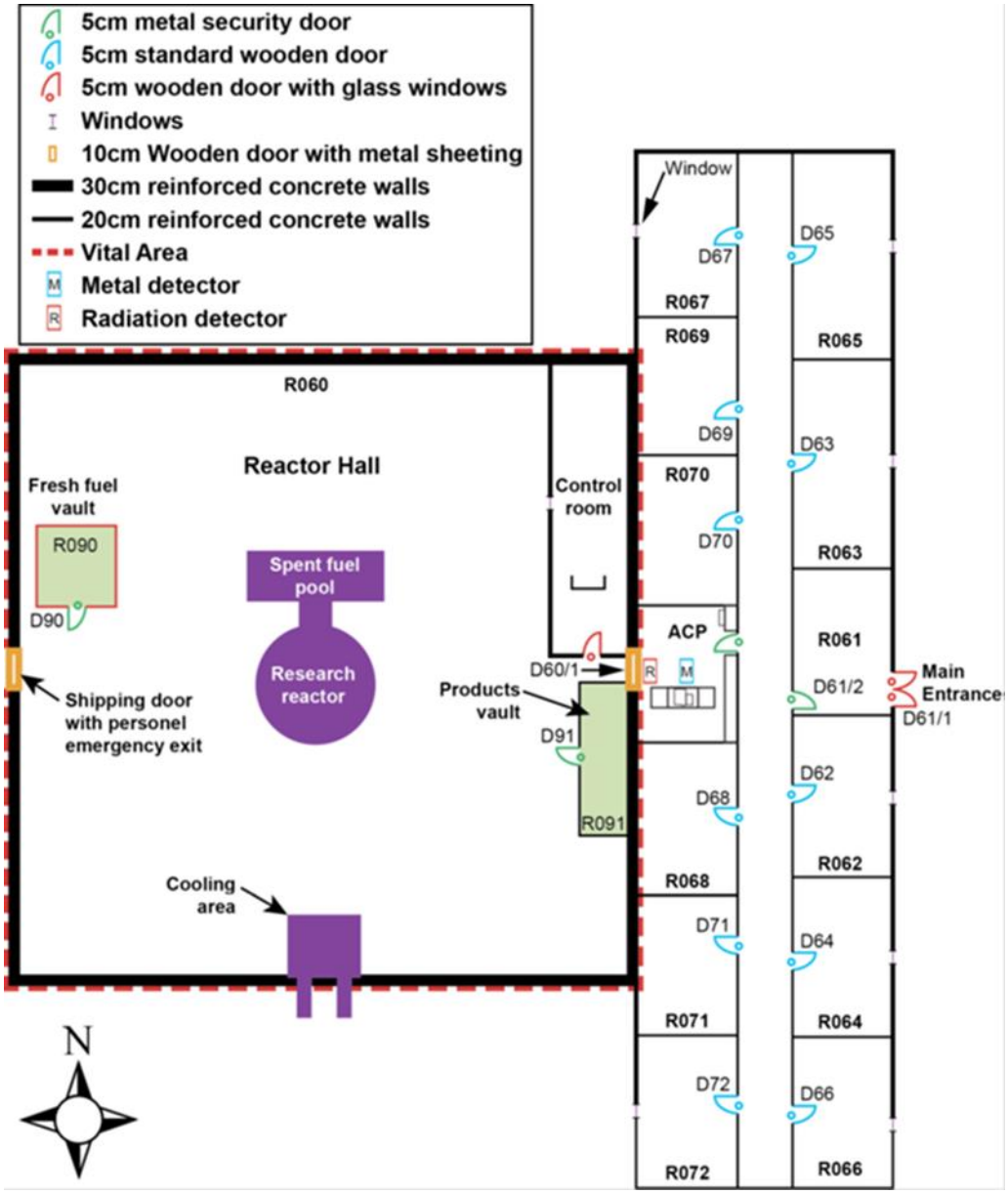


*Figure 3: Research Reactor Building Floor Plan*

**The new research reactor building floor plan:**


*Figure 4: The New Research Reactor Building Floor Plan*

# V. Conclusion

We have used the *Hypothetical Facility Data Book: The Shapash Nuclear Security Research Institute (SNRI)* as an educational tool to put theoretical nuclear security knowledge into practice. We believe that working on this data book allows for the development of critical thinking skills that are needed in the field of nuclear security. In this paper we identified many different security measures and their weaknesses related to the institute's location, the Administrative Area, the Protected Area, and the Instrumentation and Control Technology system within the SNRI. We proposed corrective actions to improve the site's protections against malicious acts, as well as a new layout for the whole site and the research reactor building, presenting the changes made using a software called Edraw Max.

# VI. Works cited

1. "Hypothetical Facility Data Book: The Shapash Nuclear Research Institute (SNRI)" (2014), , doi:10.2172/1090700.

2. Atomic Energy Licensing Board, "Guidelines for Site Selection for Nuclear Power Plant" (LEM/TEK/63, Selangor Darul Ehsan, 2011), (available at https://www.standards.doe.gov/standards-documents/1100/1194-astd-2011/@@images/file).

3. OPEN-LMS: Nuclear Security of Materials and Facilities, (available at http://elearning.iaea.org/m2/course/index.php?categoryid=102).

4. Nuclear Reactor Access Zones (2001). *Union Concerned Sci.*, (available at https://www.ucsusa.org/nuclear-power/nuclear-plant-security/nuclear-reactor-access-zones).

5. International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats,* International Atomic Energy Agency, Vienna, 2008, *IAEA Nuclear Security Series No.8*.

6. International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/revision 5)*, IAEA, Vienna, 2011, *IAEA Nuclear Security Series No. 13*.

7. Nuclear Materials Control and Accountability (2011). U.S. Department of Energy, Washington, D.C.20585

8. INMM - Nuclear Material Protection, Control and Accountability, (available at https://www.inmm.org/Technical-Resources/Best-Practices/Nuclear-Material-Protection,-Control-and-Accountab).

9. *Nuclear security culture*, International Atomic Energy Agency, Vienna, 2008, *IAEA Nuclear Security Series No.7* .

10. Computer Security at Nuclear Facilities (2011), International Atomic Energy Agency, Vienna, 2011, *IAEA Nuclear Security Series No.17.*