



**International Conference on Physical Protection of Nuclear
Material and Nuclear Facilities, IAEA Vienna, Austria
13 – 17 November 2017**

**Intrusion Detection Measures Against Insider Threats In
Al-Tuwaitha Nuclear Site**

**Asaad R. Saihood
Ministry of Science and Technology
IRAQ**

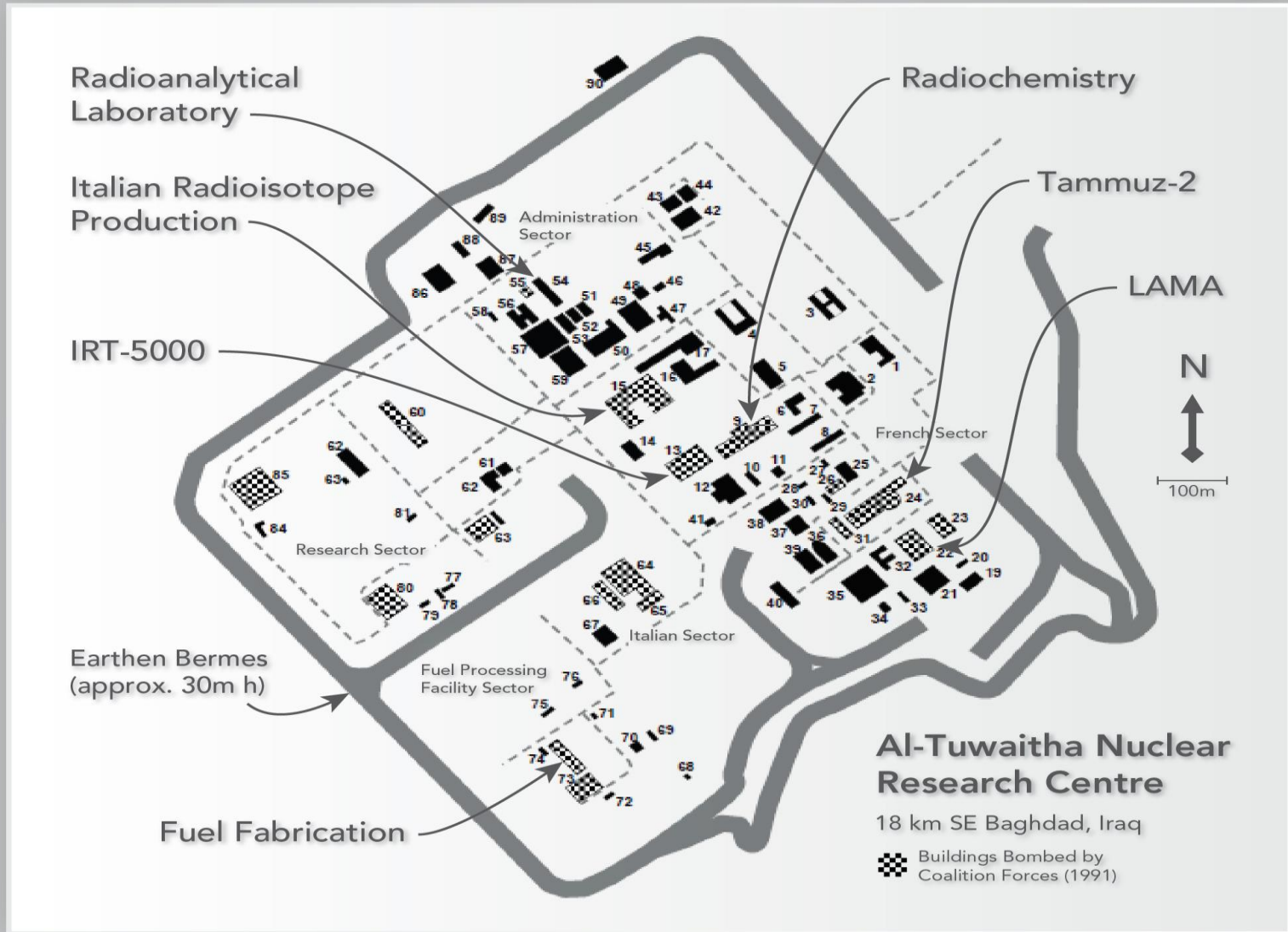
Contents

- Description of **Al-Tuwaitha Site**.
- Potential threats inside the site.
- The responsibilities of the Nuclear Security staff.
- The measures adopted.
- Upgrade PPS .
- Security Emergency plans.


The Purpose of Study

- Effectiveness and weaknesses.
- Hostile categories.
- Responsibilities
- Upgrading systems.

Al-Tuwaitha nuclear site



Potential threat categories

- Employees
 - Former Employees
 - Contractors
 - Consultants
 - Suppliers
 - Guests
- 
- Visitors

Measures taken with the visitor

- Inspection
- visitor badge.
- security record,
- visitor escort



Security team responsibilities

- Ensure the protection of workers and property
- Confidentiality of information
- Prevent sabotage and thefts
- nuclear security culture
- Collecting and documenting Personal data
- Regulation of unauthorized entry
- Periodic assessment
- Preparing statistics and data quarterly for radiation sources.

Banker B (Sources Storage)

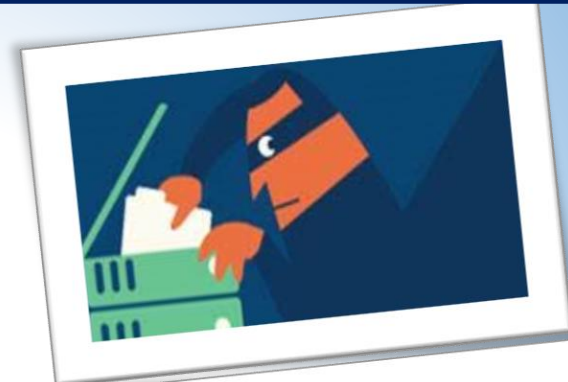


Banker-B Storage for radioactive sources.

Potential threats types inside the site

The potential risks at the **Al-Tuwaitha** site are human risk type as well as incidental risk as follow :

- Stealing
- Sabotage
- Spyware
- Terrorist activity



Theft prevention measures

- Investigations
- Follow-up of transport of materials and equipment
- periodic inventory.
- Follow up the entry and exit of materials to and from the site.
- **Declaration of crimes**



The general measures Related insider

1- Prevention

- Identity verification.
- Escort and surveillance of infrequent workers and Visitors.
- Security awareness.
- Confidentiality (security of information.
- Employee satisfaction.
- Physical division of areas.
- Sanctions (disciplinary actions and prosecution).

Protection

- Surveillance
- Access control - to prevent or detect unauthorized entry and exit.
- Inspection
- Inspections and audits for nuclear material on exit.
- Monitoring operational conditions.
- Routine testing, maintenance, and requalification of equipment.
- Protection of spare parts.
- Delay – personnel, procedures, physical barriers.
- Response (Security Emergency plans).

Satisfaction and motivation

- Financial incentives
- Health insurance.
- full services.
- Preparation of internal and external training courses.



Upgrade and Enhancements

1. Protected Area Main Gate
 - Guard House
 - Pedestrian Access
 - Vehicle Access
2. Radioactive Waste Complex
3. Bunker B
4. Communications Equipment

Guard House

- Video Management System
- Computer with Video Management System (VMS) software
- Badge printer with badges (for 2,000 employees)
- Access Control System (ACS alarm panel)
- Uninterruptible Power Supply (UPS), computer, badge readers and ACS
- Alarm annunciator (siren with strobe light)

Pedestrian Access

Entry Control Point – Pedestrian Access

- X-ray machine for scanning (1)
- Portable handheld explosives detector (3)
- Turnstile gates, bi-directional (3)
- PIN card readers (6)
- Uninterruptible Power Supply (UPS), badge readers, and turnstiles

Vehicle Access

- PIN card readers (2)
- Drop-Bar Vehicle Gates (2 , one for entry, one for exit)
- Uninterruptible Power Supply (UPS), badge readers and drop-bars
- Digital outdoor IP cameras (2)
- Outdoor lighting (2)

Radioactive Waste Complex

- Turnstile gate, bi-directional (1)
- Proximity & PIN card readers for the access control (2)
- UPS for 4 hrs. backup
- Portal Metal Detector

Radioactive Waste Treatment Station
(back view).



The ceiling area



Radiation source storage (Bunker B)

- Intrusion and hold-up alarm system with emergency and panic duress button (1)
- Outdoor lighting (2)
- 1 unit IP phone handset (VoIP)

Communications Equipment

- Fiber optic cable
- Required hardware (e.g. converters, routers)
- Network and other signal cables between gates, card readers, ACS, etc.
- VoIP handsets (3)

Security Emergency plans

- The security team has been formed for the establishments capable of facing the challenges that threaten the security of the site consists of:
 - Security director:
 - Security Officer:
 - Security personnel and supervisors:
- provide equipment
- practical exercises

Conclusions and recommendations

- A physical protection system should be designed to be effective against sabotage scenarios and terrorist threats and be consistent with the level of site protection, particularly nuclear materials.
- Prepare a contingency plan for fire and evacuation and define the terms of reference of the crisis management team.
- The need to establish an on-site operations room to manage and organize security tasks.
- Application smart card system when entering from the main gates.
- The need to review the laws on the punishment of prying employees

Conclusions and recommendations

- Provide the site with electrical generators commensurate with the size of the requirements to be redundant in case of main power outages for the continuance of the work of internal security systems.
- The need to provide important areas in the site sensors with high technology and modern work to detect penetration and infiltration and deal with it automatically.
- Continue the practical exercises for emergencies of the responsible security teams. In addition Rehabilitation, training, and guidance of security personnel and workers on safety and security procedures.

*Thank you
for attention*