

Nuclear Security Incident Analysis

Towards an Integrated and Comprehensive Approach

Presented by Robert Wesley

Office of Nuclear Security, IAEA

Authors: Richard Hoskins, Viacheslav Turkin, Robert Wesley



IAEA

International Atomic Energy Agency

IAEA Information Systems for Nuclear Security Incidents

- *Illicit Trafficking Database (ITDB)*
 - Established in 1995
 - Official reporting and collection of open source information
 - Scope covers situations where any type of nuclear or other radioactive material is outside legitimate control

The screenshot displays the ITDB interface. The top section shows a list of incidents with columns for Incident ID, Location, Country Code, Date, Incident Type, and Incident Status. Below this, a detailed view of an incident is shown, including incident data, nuclear material details, and other material information.

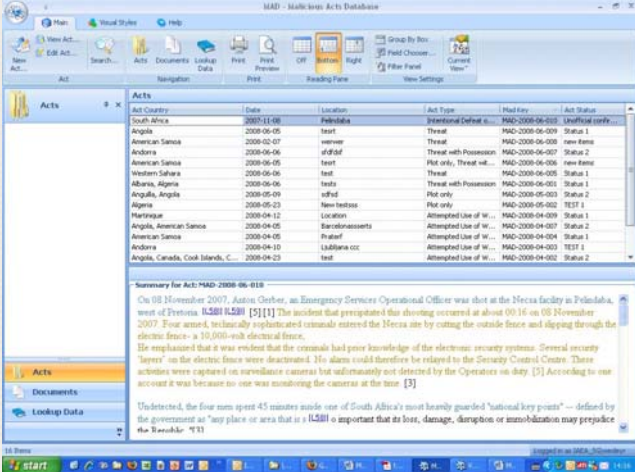
Incident ID	Location	Country Code	Date	Incident Type	Incident Status
1993-01-001	Libya	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-002	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-003	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-004	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-005	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-006	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-007	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-008	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-009	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for
1993-01-010	Yemen	RU	1993-01-01	Unaccounted for	Unaccounted for

The screenshot displays the ITDB interface showing search results. The table lists incidents with columns for Incident ID, Incident Country, Incident Date, Incident Date, Incident Type, Incident Status, and Incident Date.

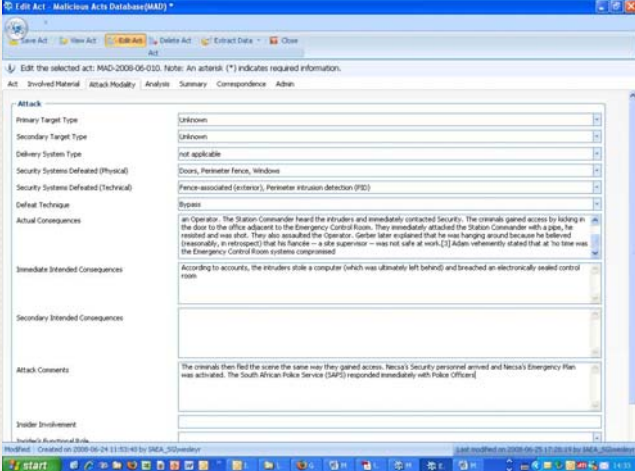
Incident ID	Incident Country	Incident Date	Incident Date	Incident Type	Incident Status	Incident Date
2001-01-001	France	2001-01-01	2001-01-01	Unaccounted for	Unaccounted for	2001-01-01
2001-01-002	France	2001-01-01	2001-01-01	Unaccounted for	Unaccounted for	2001-01-01
2001-01-003	France	2001-01-01	2001-01-01	Unaccounted for	Unaccounted for	2001-01-01
2001-01-004	France	2001-01-01	2001-01-01	Unaccounted for	Unaccounted for	2001-01-01
2001-01-005	France	2001-01-01	2001-01-01	Unaccounted for	Unaccounted for	2001-01-01

IAEA Information Systems for Nuclear Security Incidents

- Malicious Acts Database (MAD)
 - Established in 2008
 - Based on open source information
 - Scope includes data on threats, attempts, plots and fully or partially executed activities, and activities related to the intentional defeat or violation of security procedures or other technical or physical security systems at related facilities.



Act Country	Date	Location	Act Type	Mail Key	Act Status
South Africa	2007-11-08	Pelindaba	Intentional Defeat of...	MAD-2008-06-010	Unofficial confi...
Angola	2008-06-05		Threat	MAD-2008-06-009	Status 1
American Samoa	2008-02-07	unspec	Threat	MAD-2008-06-008	New Item
Andorra	2008-06-06	atfufuf	Threat with Possession	MAD-2008-06-007	Status 2
American Samoa	2008-06-05	test	Plot only, Threat with...	MAD-2008-06-006	New Item
Western Sahara	2008-06-06		Threat	MAD-2008-06-005	Status 1
Albania, Algeria	2008-06-06	test	Threat with Possession	MAD-2008-06-001	Status 1
Angola, Angola	2008-05-09	atfufuf	Plot only	MAD-2008-05-003	Status 2
Algeria	2008-05-23	New testbase	Plot only	MAD-2008-05-002	TEST 1
Marshall	2008-04-12	Location	Attempted Use of W...	MAD-2008-04-009	Status 1
Angola, American Samoa	2008-04-05	Sanctionsassets	Attempted Use of W...	MAD-2008-04-007	Status 2
American Samoa	2008-04-05	Pratuf	Attempted Use of W...	MAD-2008-04-004	Status 1
Andorra	2008-04-10	Ludlana cc	Attempted Use of W...	MAD-2008-04-003	TEST 1
Angola, Canada, Cook Islands, C...	2008-04-23		Attempted Use of W...	MAD-2008-04-002	Status 2



Act: MAD-2008-06-010

Involved Material: Attack Modality: Analysis: Summary: Correspondence: Admin

Attack	
Primary Target Type	Unknown
Secondary Target Type	Unknown
Delivery System Type	not applicable
Security Systems Defeated (Physical)	Doors, Perimeter Fence, Windows
Security Systems Defeated (Technical)	Fence-associated (electronic), Perimeter Intrusion Detection (PID)
Default Technique	Bypass
Actual Consequences	An Operator. The Station Commander heard the intruders and immediately contacted Security. The criminals gained access by locking in the door to the office adjacent to the Emergency Control Room. They immediately attached the Station Commander with a rope, he resisted and was shot. They also assaulted the Operator. Gender later explained that he was hanging around because he believed (reasonably, in retrospect) that his fiancée - a site supervisor - was not safe at work. [2] Admin retrospectively stated that at no time was the Emergency Control Room systems compromised.
Immediate Intended Consequences	According to accounts, the intruders stole a computer (which was ultimately left behind) and breached an electronically sealed control room.
Secondary Intended Consequences	
Attack Comments	The criminals then fled the scene the same way they gained access. Necsa's Security personnel arrived and Necsa's Emergency Plan was activated. The South African Police Service (SAPS) responded immediately with Police Officers.
Intruder Involvement	



Evolution of Programme

- Scope of ITDB has broadened and its objectives expanded
- Increasingly vigorous outreach programme for ITDB to enhance the comprehensiveness and quality and to recruit new State participants
- The ITDB-MAD system will provide for better trending, assessing the effectiveness of Agency recommendations, and the identification and evaluation of potential vulnerabilities, threats, and other risks.

Examples of Incident Analysis: Size of the Problem

- From 1993-2008, ITDB recorded 1562 incidents reported by States, while a further 1200 (approx) collected from open sources but yet to be confirmed by the States involved
- MAD currently contains reports on approx 200 incidents since the 1960s
- Number of incidents recorded understates the real problem

Examples of Incident Analysis:

Threat of Nuclear Terrorism

- Terrorists have shown interest in and/or attempts to acquire nuclear and radioactive materials
- Missing, unrecovered materials are cause for concern
- Involvement of buyers, criminal groups, and 'repeat offenders'
- Various groups and individuals of disparate backgrounds and motivations involved in malicious acts
- Need for frameworks for understanding drivers and inhibitors

Examples of Incident Analysis: Assessing Vulnerabilities

- Materials:
 - Category 4 and 5 radioactive sources are also a problem
- Facilities:
 - Pre-conversion, conversion, and facilities fabricating and/or handling low enriched uranium fuels have been vulnerable to theft
 - Power reactor complexes have been the targets of majority of the acts involving facilities recorded in MAD

Examples of Incident Analysis: Assessing Vulnerabilities

- Detection Architecture:
 - Detection equipment is effective in detecting inadvertent movement of radioactive materials across borders, e.g. point sources inside metal scrap or contaminated materials
 - However, the smuggling of materials has posed difficulties for such systems

Examples of Incident Analysis: Insider Threat

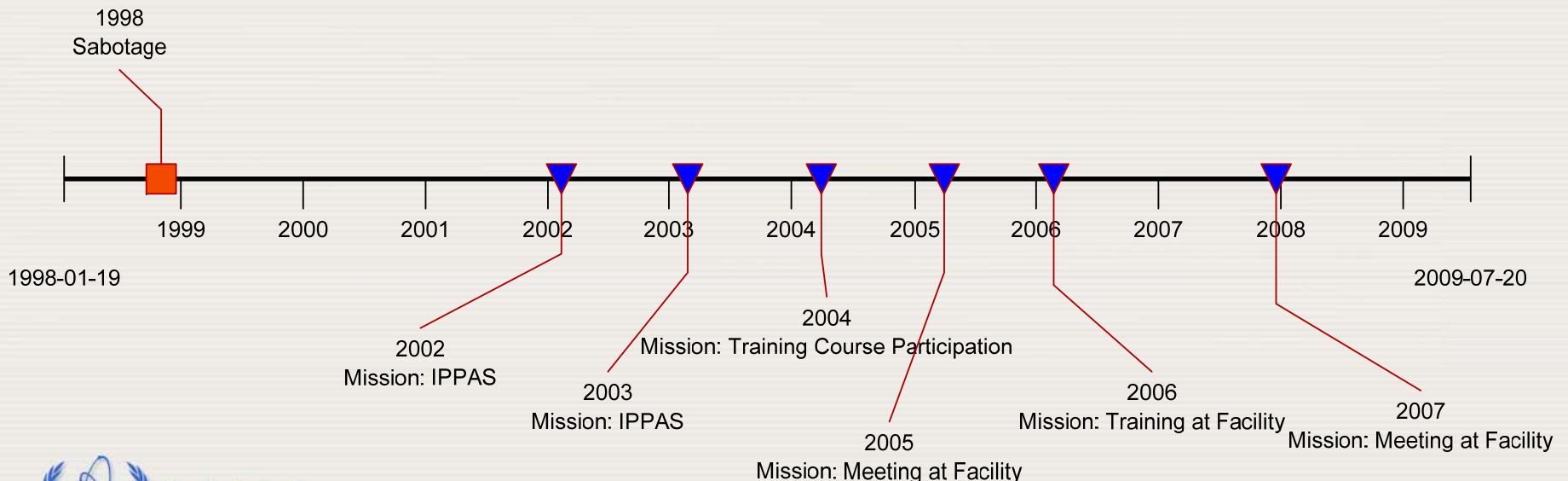
- Thefts of materials committed by insiders, including two thefts of HEU in 1994 and 1995
- Correlation between insider collusion and attempted malicious use (primarily attempted sabotage) of facilities
- Need to collect specific details related to insider acts

Further Applications of Analysis

- Inform the Agency's capacity building and other assistance programmes (e.g. International Nuclear Security Advisory Service missions)
- Cases studies and analytical findings applied to training activities and the development of guidance and recommendations documents

Further Applications of Analysis

- Inform threat assessments and designing advanced methodologies
- Input to planning facility-specific evaluation and assistance missions



IAEA Nuclear Security Plan 2010-2013

- Investing in the future of incident analysis
- Focus on improving the quality and comprehensiveness of data reported to the ITDB-MAD
- Integration of Incident analysis throughout programme of activities