System Evaluation Methods in practice for insider mitigation

Eldar Nikhanov
International Atomic Energy Agency, Vienna International Centre P.O. Box 100, A-1400 Vienna, Austria
enikhanov@kazatomprom.kz

1. Goal of the present work

In accordance with NSS 8, this work reveals approaches to providing measures of protection against an insider and a method for evaluating them in practice

2. Detection: security system

Protective measures
- **Detection**
  - **Security system**
  - Personnel surveillance
  - Monitoring of processes
  - Access control
  - Sudden inspection
- Delay
- Response
- Emergency plans

- Checkpoints for employee & vehicles, fence & gate
- Perimeter detect & alarm systems
- Overall CCTV system
- Access control system
- "Pass Office"
- Monitoring assessment center
- Guard service

2.1. Detection: personnel surveillance

Protective measures
- **Detection**
  - Security system
  - **Personnel surveillance**
  - Monitoring of processes
  - Access control
  - Sudden inspection
- Delay
- Response
- Emergency plans

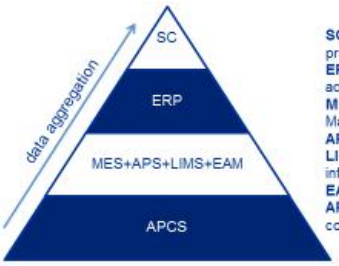
Two persons rule
- two experienced persons to monitor one another
- at least two persons be present in a sensitive area in order for each person to verify that all actions are performed as authorized
- managers should ensure that the members of such two person teams are rotated

CCTV system
- no "dark" areas
- monitoring assessment center (24/7)
- alarm system & industrial safety system integration

Access control system
- different access right
- employee's track record

2.2. Detection: monitoring of processing

Protective measures
- **Detection**
  - Security system
  - Personnel surveillance
  - **Monitoring of processes**
  - Access control
  - Sudden inspection
- Delay
- Response
- Emergency plans



SC - visualization of key production processes (>500)
ERP - financial planning and accounting
MES - Production Management
APS - operational planning
LIMS - laboratory information system
EAM - service, spare parts
APCS - automated process control system

2.3. Detection: access control

Protective measures
- **Detection**
  - Security system
  - Personnel surveillance
  - Monitoring of processes
  - **Access control**
  - Sudden inspection
- Delay
- Response
- Emergency plans

- different access right
- tighter access rights in depth
- metal, nuclear materials, explosives detectors at the checkpoints
- access to the rooms (stage) only for employees of this rooms
- protect "Pass Office"
- device identification interference in sensitive equipment, containers with nuclear material

different color of clothes & pass for employees & contractors with different levels of access

2.4. Detection: sudden inspection

Protective measures
- **Detection**
  - Security system
  - Personnel surveillance
  - Monitoring of processes
  - Access control
  - **Sudden inspection**
- Delay
- Response
- Emergency plans

- physical inventory NM every quarter
- digital NMAC system
- interference identification device integrity check
- 3 level of inspections: operator, authority body, IAEA
- testing and maintenance of industrial equipment

3. Delay

Protective measures
- Detection
- **Delay**
- Response
- Emergency plans

PHYSICAL BARRIERS WON'T HELP

Personnel
- security guard (patrol)
- operating stuff
- 24/7 CCTV assessment center

Procedures
- two persons rule
- access control instruction

Equipment
- locks on the valves, switchboards and etc.
- equipment redundancy

4. Response

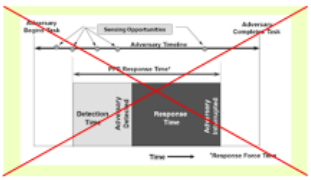
Protective measures
- Detection
- Delay
- **Response**
- Emergency plans

Security stuff
- investigation instruction
- accident response plan (access limitation, evidence preservation and etc.)
- incident notification scheme (quick alarm transmission)

Employee
- alarm transmission procedures (quick alarm transmission)
- accident response plan (mitigation of consequence)
- emergency plan

Equipment
- CCTV system recording 60 days (for investigation)
- access control system's event log (for investigation)
- available alarm system (quick alarm transmission)

Doesn't work



5. Assessment

Assessment
- **Vulnerability analysis**
- Authority body

Determining threats
- theft of nuclear materials (NM)
- dispersion of NM, including, by means of an explosion
- damage of equipment
- interference with the work of IT-systems
- damage of PPS

Critical elements	Basic threats	Type of insider	Access areas
finished products warehouse	theft of nuclear materials	2	Particularly important area

Determination of the insider model (example)

Number	Vehicle	Weapons	Equipment	Motivation	Tactic
1-2 persons	Cargo	Not required	For breaking locks	Personal and selfish	Silence

Possible actions of insider considering determining threats
- identifying detail route to realize the threat