Technologies and Institutions for Nuclear Security

Matthew Bunn
Managing the Atom "Nuclear 101"
8 May 2013
http://www.managingtheatom.org

The agenda

- Part I: Technologies
  - The problems to be solved
  - Assessment approaches
  - Physical protection
  - Material control
  - Material accounting
- Part II: National regulation and policy
- Part III: The international framework

July 2012: Protester intrusion at Y-12

- 3 protesters – including an 82-year-old nun – penetrated to the wall of the building where 100s of tons of HEU is stored
- Failings:
  - New intrusion detection system had been setting off huge numbers of false alarms
  - Cameras that could have assessed alarms had been broken for months
  - Guards assumed alarms were false; guards inside building assumed protesters' pounding was construction they had not been told about
- Root causes and lessons learned:
  - Profound breakdown in security culture
  - Difficult problem to keep guards motivated when attacks never happen
  - Every organization handling nuclear weapons and weapons-usable materials needs intensive program to assess, improve security culture, regular tests, assessments of real security performance

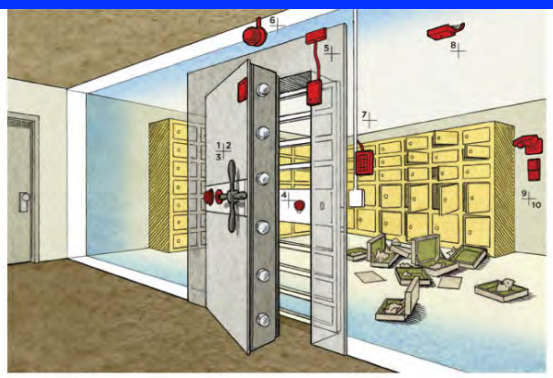
3

Antwerp Diamond Center Heist, 2003

Source: *Wired*

4

Antwerp Diamond Center Heist, 2003 (II)



The Door
1. Combination dial (0-99)
2. Keyed lock
3. Seismic sensor (built-in)
4. Locked steel grate
5. Magnetic sensor
6. External security camera

The Vault
7. Keypad for disarming sensors
8. Light sensor
9. Internal security camera
10. Heat/motion sensor (approximate location)

Source: *Wired*

5

Nuclear security: what are we talking about?

- IAEA Definition:

"The prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities."

- Focus of this talk is a subset of this broader definition:
  - How to keep nuclear weapons and the materials needed to make them from being stolen?
- This talk assumes that nuclear theft and subsequent nuclear terrorism are real dangers to the entire international community
  - See, for example, www.nuclearsummit.org

Part I: Technologies
A systems approach to nuclear security

- Define what threat is to be defended against
- Specify what targets are to be defended
- Design and build a system capable of defending the targets against the threat
- Assess the system – expert judgment, computer analyses, realistic performance tests – can it in fact defeat capable and intelligent adversaries?
- Design and build fixes to identified vulnerabilities, assess again (repeat as needed)
- Operate the system
- Human factor critical: maintain high "security culture," based on awareness of the threat

The design basis threat (DBT)

- Design basis threat is the threat systems are required to be able to defeat:
  - How many outsiders?
  - How many insiders?
  - How many teams?
  - How well trained?
  - How well equipped and armed (automatic weapons? Night-vision goggles? RPGs? Shaped-charge explosives? Armor-piercing bullets?)
  - What kind of vehicles?
  - What kind of tactics and strategy?
  - What motivation? Willing to die?

Demonstrated outsider threats

- Large overt attack
  - e.g., Moscow theater, October 2002: ~ 40 heavily armed, well-trained, suicidal terrorists, striking without warning
- Multiple coordinated teams
  - e.g., 9/11/01 -- 4 teams, 4-5 participants each, well-trained, suicidal, from group with access to heavy weapons and explosives, >1 year intelligence collection and planning, striking without warning
- Significant covert attack
  - e.g., Indian incident with thieves drilling through wall for sources
- Use of unusual vehicles
  - e.g., helicopters used in many recent jail escapes
  - e.g., speedboat planned for use in $200M Millennium Dome theft

Demonstrated insider threats

- Multiple insiders working together
- Often including guards
  - Most documented thefts of valuable items from guarded facilities involve insiders – guards among the most common insiders
  - Goloskokov: guards "the most dangerous internal adversaries"
- Motivations:
  - Desperation
  - Greed/bribery
  - Ideological persuasion
  - Blackmail

A trustworthy employee may not be trustworthy anymore if his family's lives are at risk

Some tactics of concern

- Deception
  - Example: Thieves dressed as police arrive at Gardner Museum, walk off with priceless Rembrandts
  - Example: Insider pulls alarm, "emergency, everybody out!" and carries material through emergency exit
- Rapid barrier breaching or avoiding
  - Example: throw a carpet over the razor wire, over the fence in seconds
  - Example: hand-carried explosives can blow through fences, vault doors, even (some) thick walls in seconds
  - Example: tunneling into facility, or flying over barriers in helicopter, hang-glider, etc.
- Conspiracy: multiple insiders, insiders+outsiders
  - Hardest threats to defeat – insiders may include guards (41% of thefts from guarded facilities in one study), security experts

What the security system needs to do

- *Detect* – setting off an alarm
  - Example: intrusion detectors on or near perimeter fences
  - Example: active seals on nuclear material container
- *Assess* – what caused the alarm?
  - Example: security cameras at perimeter, critical points throughout the facility
- *Communicate* – "Ten bad guys are breaking in! Go to the north fence to stop them!"
- *Delay* – slow the bad guys down until the cavalry can come over the hill
- *Defeat* – get a response force to the scene fast enough, that is capable enough, to arrest, shoot, etc. the bad guys before the bad guys have an opportunity for catastrophic harm

Modeling the layers of the protection system

Figure 17–2. Basic Areas At An Example Facility

Multiple Possible Adversary Pathways Through Each Layer

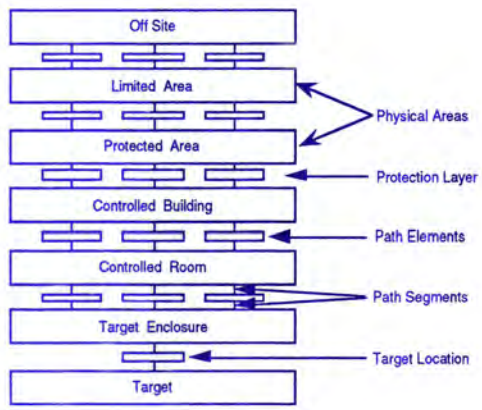


Figure 17–7. ASD Concept

Estimating probability of adversary sequence interruption – each pathway

Estimate of Adversary Sequence Interruption	Prob. of Guard Comm.		Response Force Time (in Seconds) Mean	SD
	0.95		300	90

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean	SD
1	Cut Fence	0	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption:	0.476

Estimating probability of adversary interruption: parsing the example

- This facility has a response force that takes 300 seconds (5 minutes) to arrive
- But the facility has no ability to detect adversaries cutting the fence – first hope of detection is when they blow through the door of the building
- After that door, it's only 220 seconds to a sabotage
- So, the protection system has less than a 50-50 shot at preventing sabotage on this pathway, against adversaries as capable as those predicted
- Possible fixes: add detection capability at the fence (likely cheapest); put in stronger vaults, etc. to increase delay time after going through door; decrease response force arrival time (e.g., move them closer to facility).

Importance of the "human factor"

- *Intelligent adversaries* will seek to identify and exploit weaknesses in the system
  - Will actively try to think of things the security planners *haven't* thought of
  - Insiders are particularly difficult to model, and to protect against: they know the system and its weaknesses (may be among the vulnerability assessors), are trusted by other employees
- *Intelligent employees* will seek to avoid doing things that are inconvenient, boring, that they perceive as unimportant, and that distract from other activities more likely to bring promotion, raises, or pleasure
  - Guards will say they patrolled, checked locks, when they didn't – when the Superbowl is on, they may be watching TV, not the fences
  - Personnel in general will disregard security rules they think are excessive or useless, and will not behave in the way that system designers may expect – has to be taken into account

Assessing vulnerability assessment

- Key issues are similar to those for probabilistic risk assessment – system too complex to predict (and get probability data on) each sequence; unforeseen system interactions and common-mode failures particularly problematic
- Even worse in the vulnerability assessment case, because of intelligent adversaries actively trying to think of things you haven't thought of
- Importance of realistic ***performance testing*** – does the system really protect, when faced with a credible adversary force (and/or insider) trying to overcome it?
- Assessment of ***absolute*** magnitude of vulnerability rarely attempted – never trust a statement that a facility is "secure", always ask "against what, and proven how?"

The need for performance testing

- Computer vulnerability assessment alone will reveal only the vulnerabilities the assessors think of
- Realistic performance tests – "red team" outsiders attempting to break in, "red team" insiders attempting to smuggle items out – can:
  - Reveal vulnerabilities that require correction
  - Convince higher-ups that more investment in security is in fact needed
  - Provide training for, increase security awareness of, guards and other security personnel
- Regular performance testing required at both DOE and NRC facilities
- Many, many issues – realism, cheating, who tests, how often, etc. – but clearly better than no testing

Importance of security culture

- If employees don't believe that the threat is real, they won't devote much effort to security measures
- If employees don't believe the security rules are sensible and effective approaches to addressing the threat, they won't follow them
- If guards turn off alarms because they are annoyed by the false alarm rate, employees prop open security doors for convenience, and guards patrol without ammunition to avoid accidental firing, even excellent hardware will not provide good security
- "Good security is 20% hardware and 80% culture."
- Strong security culture is hard to achieve (example: recent Y-12 intrusion)

Security culture matters: Propped-open security door

Source: GAO, Nuclear Nonproliferation: Security of Russia's Nuclear Material Improving, Enhancements Needed (GAO, 2001)

21

Perimeter fences and intrusion detection

- Effective system typically has two fence layers, with clear area between
- Fences themselves usually provide little delay
- Intrusion detectors
- Security cameras
- "Perimeter Intrusion Detection and Assessment System" (PIDAS)
- Expensive – in U.S., PIDAS costs >$3000/m, $3M for 1 km bunker fence, ~10%/yr for O+M

Intrusion detectors -- detection

- Examples: taut wire, microwave, infrared, etc.
- Each subject to different kinds of false alarms, means of defeating
- Best systems usually have two independent types of sensors
- Guards patrolling perimeter can also serve as detectors
- Guards in guard towers: only ~30% detection probability

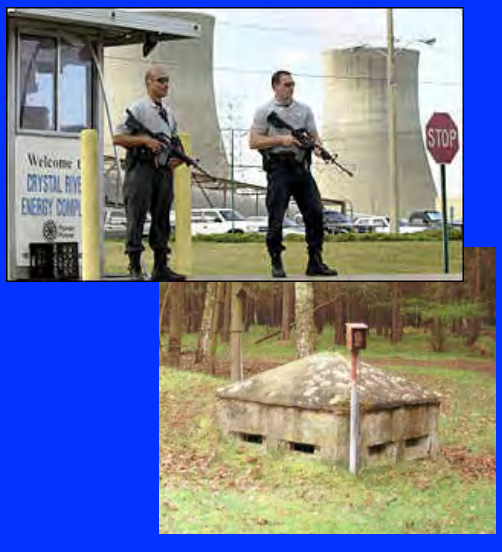
Cameras, people -- assessment

- Security cameras traditional – images viewed from central alarm station
- Guards can be sent to assess alarm also
- Adversaries may cause multiple alarms, temporary blinding of cameras, exploit spots with broken cameras…
- Only after assessment suggests attack is underway does timeline for response begin

Barriers -- delay

- Examples: fences, walls, vaults, metal tie-downs
- Many barriers provide few seconds-2 minutes delay against terrorists with shaped charge explosives
- Barriers also help keep adversaries in the open long enough to fire on them
- Newer technologies: sticky foam, cold smoke

Protective forces -- defeat



- Typical arrangement: small force on-site, larger response force some distance away – can they get there in time?
- Response forces must have adequate numbers, armament, training, equipment, fighting positions to defeat adversaries
- Guards in exposed positions likely to be shot – but in bunkers highly effective

Access control

- Purpose: allow only trusted insiders into sensitive areas, and only in accordance with rules (e.g., two-man rule)
- Based on something you have (e.g., key), something you know (e.g., password), something you are (e.g., photo, fingerprint, retina scan)
- Guards checking photo IDs minimally effective – IDs readily faked, guards attention wanders

Personnel screening and reliability

- Access control has limited value unless effective screening of personnel is in place
- Typical approach: background check before hiring (criminal record, terrorist links, financial status, comments from neighbors, co-workers, others)
- Some organizations also use: polygraph (generally ineffective), psychological interviews (probably ditto)
- Continuing checks after hiring also important:
  - Drug and alcohol testing
  - Monitoring of on-the-job performance, reporting of irregularities, suspicious activities
  - Regular monitoring of, e.g., financial status (most major spy cases in U.S. financially, not ideologically, motivated)
  - Re-investigation every few years (e.g., every 5 years for U.S. "Q" [nuclear weapons information] clearance)

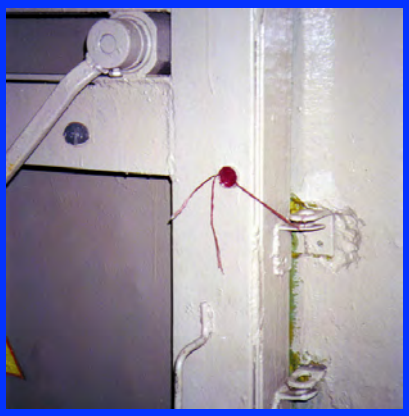
Material control – detecting material removal (ideally in real time)

- Security cameras in all nuclear material areas
- Variety of other sensors (as with exterior detectors)
  - Example: Sensor monitors weight of nuclear material in cans on shelf, sets off alarm if weight goes down
- Tags and seals:
  - Example: Active RF seals – instant radio report if tampered with
- Nuclear material detection at doors to key areas (portal monitors)
- Vaults, access control, 2-man rule

Material control – tags and seals

- Tags intended as unique identifiers – dummy can't be substituted
- Seals intended to reveal tampering
- IAEA applies hundreds of seals/yr, thousands used in national programs
- Many types – most can be defeated, with varying degrees of difficulty
- Recent ideas: combine tag/ seal with continuous video monitoring

Ineffective padlocks and seals for nuclear material in Russia



Material control – portal monitors

- The best available pedestrian portal monitors are generally effective – though not perfect
- Passive gamma detection
- More difficult to detect material (esp. HEU) in cars, trains, containers
- Many facilities also have metal detectors, X-ray of bags, at least going in (to limit ability to bring in guns or explosives)

Securing transports

- Inevitably more difficult – no fixed barriers for delay, no detection until attack begins
- Nuclear fuel transported in heavy armored casks
- Nuclear weapons in specially designed armored trucks
- Risk can be lowered with investment in security force to accompany
- Some current shipments lightly guarded

"Inherently secure" systems?

- Examples: concrete blocks ("BFRs"), steel cages
- Less reliance on human factor, security culture
- No need for continuing investments for sustainability
- Only applicable for rarely used material
- Only provide delay – not detection or defeat
- Can be highly effective (and cheap) in concert with other system elements

Material accounting

- Purpose: detect removals (after the fact), or confirm that no significant removals have occurred
- Wide range of measurement systems available
- Irreducible uncertainties always exist
- "Protective forces fight the fight, but MC&A tells you who won"

Material accounting (II)

MUF (*M*aterial *U*naccounted *F*or) =
Beginning inventory
+ Additions to inventory
- Ending inventory
- Removals from inventory

- σ^2**MUF** -- standard deviation of MUF -- is measurement precision
- If MUF > than some threshold level -- usually **3** σ^2**MUF** -- IAEA rejects the hypothesis that real MUF is zero, investigates possibility that diversion has occurred
- For item facility (e.g., LWR), MUF=0 unless something is missing

Material accounting (III)

Tools of Material Accountancy

- *Destructive Analysis* – Take a chemical sample of the material to laboratory for analysis. Highly accurate, but expensive and long delays.
- *Non-Destructive Analysis (NDA)* – Estimate content of U235 or Pu239 by measuring mass, heat, gamma emissions, neutron emissions, transmissivity (e.g., k-edge densitometer), other properties, using portable or on-site equipment. Passive (measure naturally occurring properties, emissions) or active (measure response to pulse of neutrons, gammas, etc.). Less accurate (typically), but far more convenient. DA can be used to calibrate and confirm the accuracy of NDA equipment.

Problem 1: Item accounting

- You are a guard at a nuclear weapons bunker. The commanding officer tells you to check to make sure no weapons are missing.
- You check the records and find that there are supposed to be 20 weapons.
- You visually count the weapons in the room and find that there are 20.
- Are you finished?

Problem 1: Item accounting

- Are you finished?
  - Check records to make sure they have not been tampered with
  - Check seals and identifiers on warheads to make sure dummy warheads haven't been switched
  - Review facility logs for all warheads that have entered and left
  - Review security camera video for all suspicious activity

Problem 2: Minimizing measurement uncertainties

- A facility dissolves a batch of nuclear material; it only partly dissolves, so they add more acid – and then add more acid again

:·	Input	Output	Difference
Batch 1	10	1	9
Batch 2 (acid added)	0	3	-3
Batch 3 (acid added)	0	5	-5

- Is the mean absolute value of MUF 5.67?

Problem 2: Minimizing measurement uncertainties

- The three batches have only one input of nuclear material – should be thought of as one batch
- Saying you have 90% MUF on the first batch, 30% on the second, and 50% on the third makes the uncertainty range so wide there's no hope of detecting diversions
- This is a real case from a U.S. facility (specific data is hypothetical)

Problem 3: Accounting by difference

- Facility accurately measures input and output of a process area
- In-process inventory in the process area is defined by output minus input.
- Is there a problem here?

Problem 3: Accounting by difference

- This practice of "accounting by difference" makes the whole accounting program pointless – if the difference between output and input is *defined* as being still in-process, rather than attempting to measure and estimate in-process material, theft of material will never be detected
- Practice was widespread in Soviet Union (e.g., output-input defined as "losses to waste"), observed in recent years at U.S. facilities, remarkably

International safeguards accounting ≠ to accounting + control for theft prevention

- Example 1: Accounting at reprocessing plant
  - May be VERY difficult for international inspectors to confirm that the operator, with the entire resources of the state, is not diverting material
  - May NOT be difficult for the operator to confirm (using knowledge of plant operations, inspection of everything entering and leaving) that small groups of insiders are not removing things
- Example 2: Security measures international inspectors don't care about
  - International inspectors don't care when diversion occurred, who had access at that moment – domestic security people do
  - International inspectors don't care if the workers leave the material out on the tables at night – domestic security people do

Example: new accounting and control system at Elektrostal

- Major HEU and LEU fuel fabrication facility in Russia
  - Site of multiple HEU thefts in 1990s
- New pilot accounting and control system:
  - Material enters area in sealed canister, accurately weighed
  - Canister can only be opened by worker using his electronic card and passcode – knows WHO opened the canister and WHEN
  - Canister only opens into glovebox where work is to be done – which automatically weighs the material again
  - Material can only be removed from glovebox into a similar canister, which can only be done using an electronic card and passcode – and it is then measured again
  - Cameras observe the entire area at all times
  - System knows where the material is, and who has access to it, in real time

Summary

- Wide range of technologies can be applied to the problem of securing and accounting for nuclear stockpiles
- Because employees may be lazy and adversaries may be clever, the problem is a very difficult one
- Price of security is eternal vigilance – which is hard to maintain when attacks never happen
- Security culture among the personnel is key – "good security is 20% hardware and 80% culture.
- Performance testing is critical – to reveal vulnerabilities, to keep people on their toes, to convince those who control resources of the need for upgrades
- Need to institutionalize mechanisms for "thinking like the bad guys."

Part II: National regulation and policy

- Various questions countries must answer:
  - What threats should nuclear weapons, HEU, and plutonium be protected against?
  - What specific security measures should be required?
  - How should these vary with the type of material, and how hard it would be for terrorists to use to produce a nuclear blast?
  - How much will it cost, and who should pay?
  - How do we strengthen security culture?
  - Who's in charge in the event of a real incident, and how do we ensure different parties involved are properly coordinated?
- Many of these are answered in regulations. Key questions:
  - Are the regulations strong enough that, if followed, effective nuclear security would result?
  - How well are the rules implemented and enforced?
  - Does the regulator have the needed authority, independence, resources, expertise, and culture?

Part III: The international framework

- Key purpose of *international* and *national* frameworks is to ensure effective *local* nuclear security
  - Focus should never be on ratifying agreements for their own sake, but on optimum ways to strengthen security on the ground
- International nuclear security framework includes many elements – "regime complex," not a single regime
  - Binding agreements
  - International recommendations
  - Technical cooperation
  - Summits and other high-level discussions
  - IAEA services
  - Requirements of supply agreements
  - Best practice exchanges
  - More…
- Constrained by complacency, sovereignty, secrecy, politics

We need more effective global governance of nuclear security

- Currently we have:
  - No international standards that specify what levels of security nuclear weapons, plutonium, or HEU (or major power facilities) should have
  - No regular international mechanism to build confidence that states are putting effective nuclear security in place
  - No forum for continuing high-level discussion of nuclear security after the summit process comes to an end
- Current patchwork of nuclear security agreements, initiatives is clearly insufficient
  - But efforts to negotiate new treaties are unlikely to succeed in a timely way
  - More likely to succeed with political commitments among groups of like-minded states

49

The international nuclear security framework is insufficient

- Binding agreements
  - 1980 Physical Protection Convention
    - » U.S. originally hoped would be effective, binding global standard
    - » Least common denominator: covers ONLY security for material in international transport – and only civilian material (~15% of total)
    - » Minimal, vague security requirements
    - » Includes extensive legal provisions, requiring all parties to pass laws making nuclear theft a crime and giving them authority to arrest and prosecute or extradite nuclear thieves from elsewhere
  - 2005 Amendment
    - » Covers civilian material in domestic use
    - » Parties must have a rule on nuclear security – but what should it say?
  - 5 Nuclear Terrorism Convention
    - » All parties to take "appropriate" nuclear security measures – unspecified
    - » Mostly focused on legal response
  - UNSC Resolution 1540
    - » All states must provide "appropriate effective" nuclear security -- unspecified

The international nuclear security framework is insufficient (II)

- International recommendations
  - IAEA "Nuclear Security Series," especially INFCIRC/225
    - » More specific, but still quite general – should have a fence with intrusion detectors, but how hard should they be to defeat?
    - » Compliance voluntary (though most countries do)
- Technical cooperation and funding
  - Nunn-Lugar, comparable programs
  - Global Partnership
  - Substantial progress – but varies greatly from site to site, country to country; many security elements can't be much influenced from outside
- Best practice exchanges
  - WINS
  - U.S.-Russia-UK, others
  - Little data on implementation, some countries do not participate

The international nuclear security framework is insufficient (III)

- Cooperative frameworks
  - Global Initiative to Combat Nuclear Terrorism
    - » 85 nations participating
    - » Helps to convince countries of reality of threat
    - » Sharing of experience, best practices, capacity-building
    - » Modest focus on upgrading nuclear security
  - Proliferation Security Initiative
    - » Unlikely to stop smuggling of suitcase-sized items
  - Nuclear Security Summits
    - » Brought together leaders from 50+ countries and organizations
    - » Elevated issue from technical experts to political leaders
    - » Commitment to secure all vulnerable nuclear material in four years
    - » Broad, general work plan focused on already-existing initiatives
    - » More specific "house gifts" and "gift baskets"
    - » What happens when the summits come to an end?

The international nuclear security framework is insufficient (IV)

- The IAEA role
  - Developing recommendations and guidance (e.g., INFCIRC/225, "Nuclear Security Series")
  - Offering peer reviews (e.g., IPPAS, INSServ)
  - Coordinating assistance (~100 countries now have "Integrated Nuclear Security Support Plan" with IAEA), peer reviews, assistance, data
  - Maintaining Illicit Trafficking Database (ITDB)
  - Convening international discussions (e.g., upcoming July 2013)
    - » Could be an important forum for continuing discussion after summits stop
  - All voluntary, mostly limited to non-nuclear-weapon states

Many tiles in the mosaic – but is it yet a beautiful picture? No common baseline of nuclear security for all Pu and HEU

Comparing governance: nuclear safety and nuclear security

- International standards
  - Safety: IAEA safety standards and guides in wide range of areas, widely respected and used, fairly detailed (e.g., instructions on how to model potential tsunami threats)
  - Security: IAEA security series just beginning, not as detailed or as widely used
- Sharing and learning from experience
  - Safety: Facilities report on incidents, root causes, lessons learned; IAEA/NEA and WANO maintain databases, analyze, and distribute
  - Security: no comparable mechanism
- Peer review
  - Safety: Several varieties of IAEA peer review services available; all power reactors members of WANO, agree to accept peer reviews
  - Security: IAEA offers peer review, only a few HEU and Pu facilities have ever had one; no industry peer reviews

54

Comparing governance: nuclear safety and nuclear security (II)

- Discussion, identifying next steps
  - Safety: Regular review meetings of the Nuclear Safety Convention; WANO meetings; many others
  - Security: Nuclear security summits – but no other comparable mechanism
- Sharing best practices
  - Safety: Extensive sharing through WANO, IAEA
  - Security: Limited sharing through World Institute for Nuclear Security
- Independent advice
  - Safety: International Nuclear Safety Group (INSAG) publishes annual letters on safety priorities, wide range of analyses and reports; many NGOs providing analysis and critique
  - Security: AdSec provides confidential advice to IAEA, does not publish reports; small number of NGOs providing analysis and critique

55

Backup slides if needed…

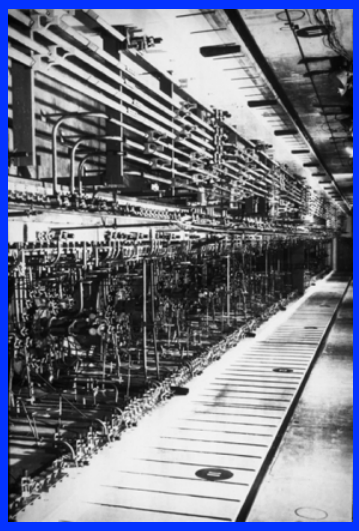
International accountancy standards

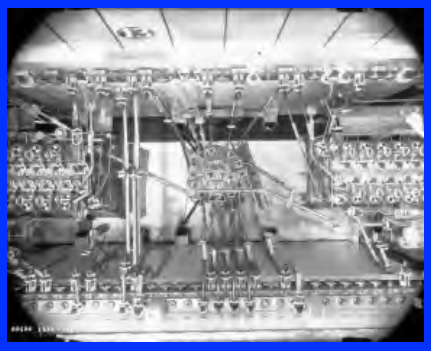
Facility Type	Relative STD (%)
Uranium enrichment	0.2
Uranium fabrication	0.3
Plutonium reprocessing	1.0
Plutonium fabrication	0.5
Scrap store	4.0
Waste store	25.0

Accountancy and inspection

- Like bank auditor, inspectors don't actually count all the money (measure all the material). Instead:
  - *examine records* provided by operator
  - inspect *statistical samples* of total quantity of material (based on the risk of the diversion they are attempting to detect) to build confidence records are accurate
  - in modern, automated facilities, often rely on in-line measurement equipment built by the operator -- premium on validating that measurements are accurate and unbiased
  - inspector must be able to make *independent judgment* -- not simply believe what the operator says
- Difference between inspector's measurements and operator's measurements is *MUF-D*

Reprocessing Plant Piping





Safeguarding a reprocessing plant

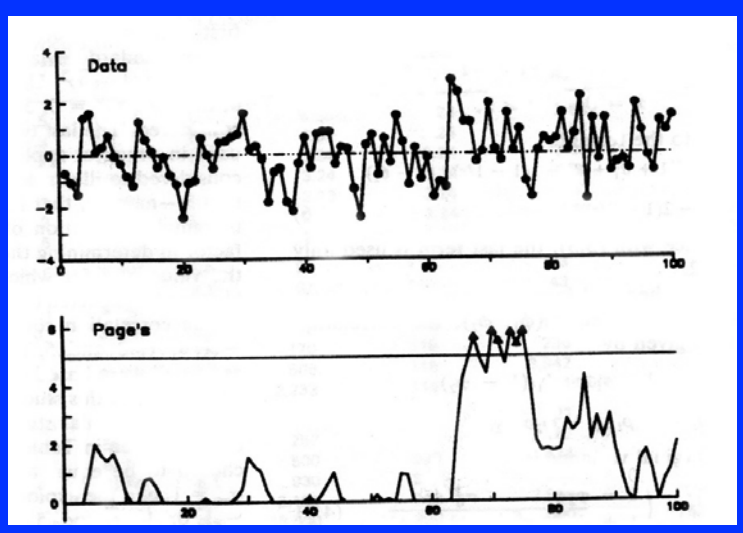
- Large commercial plant: 800 MTHM/yr, ~8 tPu/yr
- 1 close-out for measured inventory/yr
- 1% uncertainty: σ MUF=80 kg Pu
- If only challenge if MUF>3 σ MUF=240 kg Pu, can't come close to meeting the significant quantity goal
- Also, can't meet the timeliness goal with 1 inventory/yr
- Partial solutions:
  - Comprehensive transparency and containment and surveillance throughout plant – monitor all flows, detect all unusual activity
  - Near-real-time accountancy – much more frequent partial measurements of material in process, with statistical models designed to detect both abrupt and protracted diversions

Safeguards technologies: A wide range

TABLE 7: VERIFICATION MEASUREMENT METHODS FOR ON-SITE IAEA ANALYTICAL LABORATORIES

PROCESS AREA	SAMPLING POINT	INSTRUMENT OR METHOD	CONCENTRATION MEASUREMENT	SAMPLE FRACTION	GOAL ACCURACY
HEAD END	INPUT TANK	HYBRID K-EDGE DENSITOMETER (HKEDG)	Pu U	100 % 50 %	≤ 1 % ≤ 0.5 %
SEPARATION	BUFFER/FEED TANKS	ISOTOPE DILUTION MASS SPECTRO-METRY (IDMS)	Pu U	25 % 2 %	≤ 0.2 % 0.2 %
SEPARATION	SCRUB AND WASTE TANKS	Pu(VI) SPECTRO-PHOTOMETRY	Pu	< 20 %	≤ 25 %
Pu PURIFICATION	COLLECTION AND FEED TANKS	HKEDG IDMS	Pu Pu	50 % ≤ 10 %	1 % ≤ 0.2 %
	PuN TANKS	KEDG IDMS	Pu Pu	25 - 100 % 10 - 90 %	0.2 % 0.1 %
	WASTE TANKS	Pu(VI) SPECTRO-PHOTOMETRY	Pu	< 10 %	≤ 25 %
U PURIFICATION	UN TANKS	K-EDGE DENSITOM-ETER (KEDGG)	U	≤ 10 %	0.2 %
	UO_2 CANS UO_2 CANNING	NDA (MEASURE-MENTS MADE IN PLANT) KEDG	U U	≤ 10 % 1 %	< 5 % 0.2 %
MOX CONVERSION	U, Pu N TANKS	KEDG	U Pu	< 10 % 50 %	0.2 % 0.2 %
		IDMS	Pu	20 %	≤ 0.2 %
	MOX CANISTERS	NDA (MEASURE-MENTS MADE IN PLANT)	Pu	100 %	1 %
	MOX CANNING	KEDG	Pu	25 %	≤ 0.2 %

Statistical tests: Can you find the diversion in the noise?



Safeguards implementation realities

From the 2002 *Safeguards Implementation Report* (courtesy of Iranian ambassador to the IAEA Salehi):

- 357 facilities under safeguards worldwide with at least 1 significant quantity (SQ) of nuclear material
- Of these, 34 facilities in 15 states failed to fully attain quantity goal (that is, safeguards would not have been able to detect diversion of an SQ with desired confidence)
- 32 facilities in 15 states failed to fully attain the timeliness goal (that is, detection might not have occurred fast enough)
- 6 facilities, quantity goal hasn't been met for years, "because the measures foreseen in safeguards approaches could not be implemented"
- 6-7 LWRs, inspections messed up by SF having already been loaded into casks before inspection

Environmental monitoring and nuclear forensics

- All nuclear facilities, no matter how well-contained, release some atoms of Pu and U – can be detected, *in principle*
- Swipes taken from walls and floors of a building can reveal in detail what isotopic mix of plutonium was separated when, what enrichments of U produced in that building
- Samples from as much as a kilometer away – pine needles, soil, etc. – can detect telltale traces of Pu or HEU
- Crystal structure, other microscopic properties can reveal where material produced