The Interface of Safety and Security in the Response to a Malicious Act

Edward Waller

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

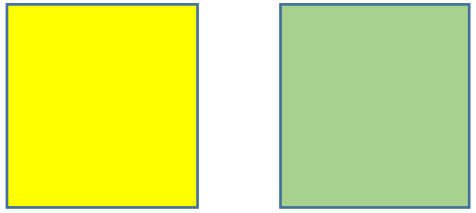
CANADA

21 April 2015

Presented at the
International Experts Meeting on Assessment and Prognosis in Response to a Nuclear or Radiological Emergency
20-24 April 2015
IAEA Headquarters, Vienna Austria

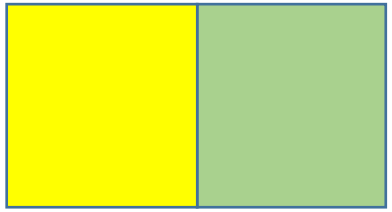
Progression of the Interface

- Where we were



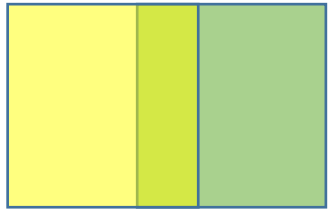
- Air gap between STEs and Gates, Guards & Guns

- Where we are



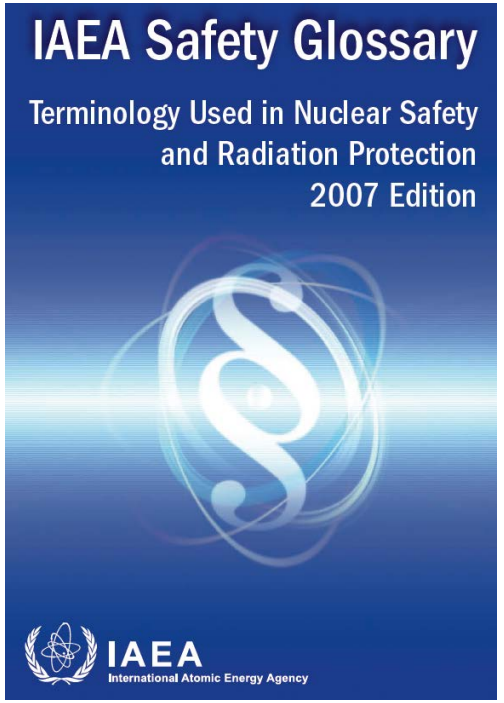
- Some level of communication and understanding of roles

- Where we should be



- Completely integrated cross-functional interoperability

Some Definitions



- (nuclear) safety
  - The achievement of proper *operating conditions*, **prevention** of *accidents* or **mitigation** of *accident* consequences, resulting in **protection** of *workers*, the public and the environment from undue *radiation* hazards.
- (nuclear) security
  - **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*
  - In general, ***security*** is concerned with *malicious* or negligent actions by humans that could *cause or threaten harm to other humans*; ***safety*** is concerned with the broader issue of *harm to humans* (or the environment) from *radiation*, whatever the cause.

Nuclear Safety

PROTECT

Nuclear Security

Is there any difference in **assessment process** or objectives if the nuclear/radiological event is a result of a malicious act versus an accident?

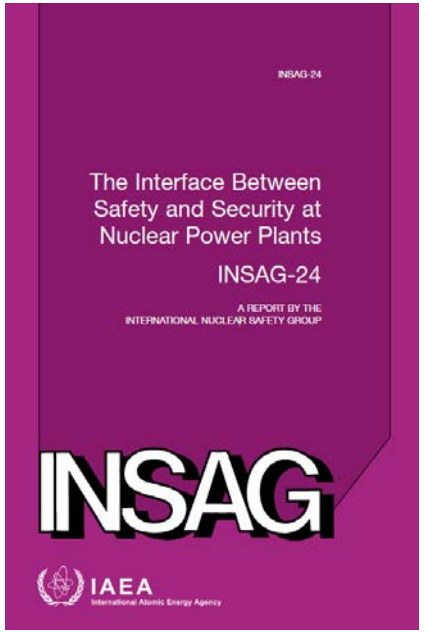
- Accident may or may not be initiated by a human, but progresses in a ‘semi-predictable’ fashion

- Malicious (hostile) act is always driven by humans, and progresses in a generally non-predictable fashion

vs.

What is the interface between the radiological emergency response organization and the security response force?

- INSAG-24: 49. The management authority for both safety and security should be centralized in the operator's organization so as to ensure appropriate coordination

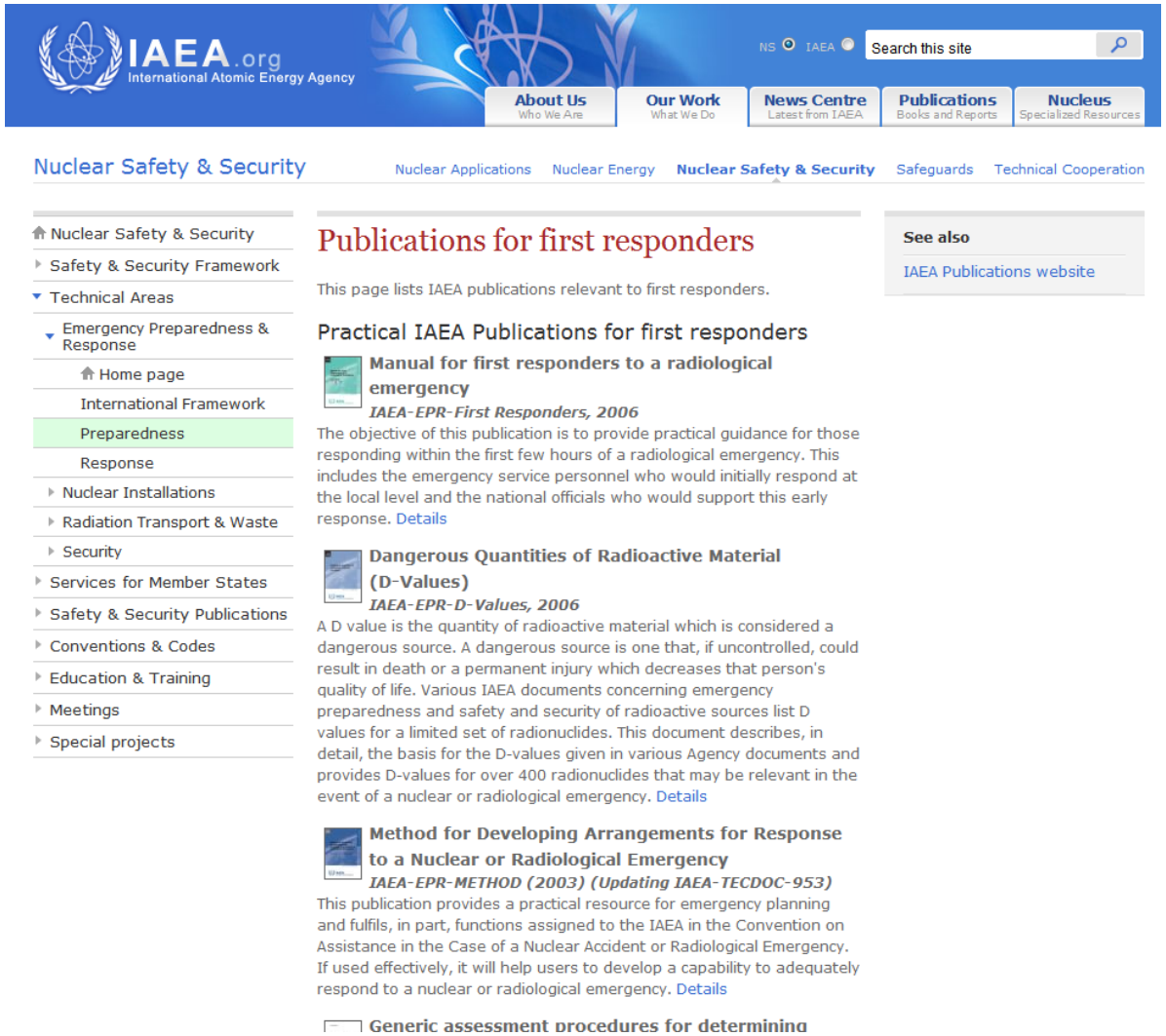


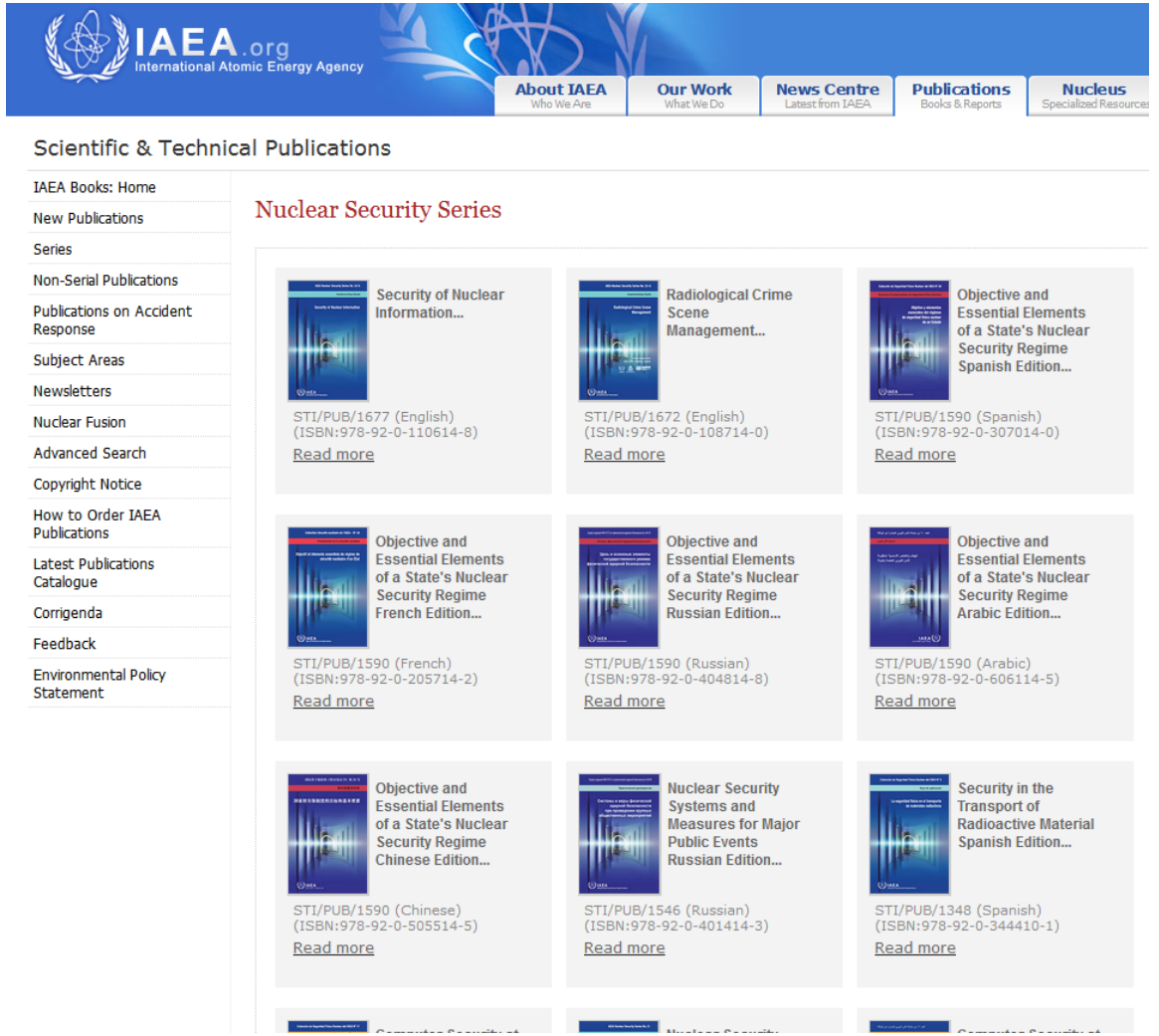
- UN NRC: Bulletin 2005-02
  - How emergency classification schemes address security events
  - Timeliness of security event notification
  - Onsite protective action plans
  - Alternate onsite emergency response facilities
  - How emergency preparedness exercises address security events

Issues to resolve for nuclear/radiological emergency response

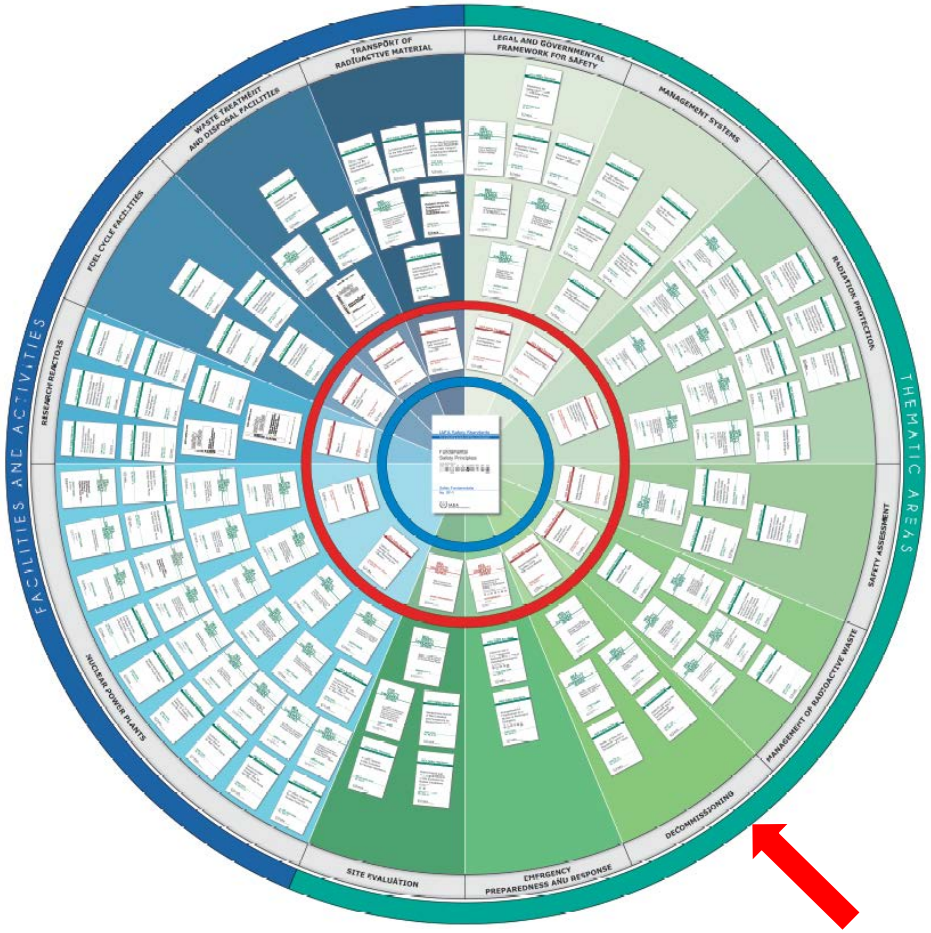
- How has the event been assessed?
  - Is an accident really an accident?
- Who takes the lead on the response?
  - Is there a coordination mechanism?
- What are the roles and responsibilities of the different emergency response groups?
  - Has the potential insider threat been addressed?
  - Is there a primary or concurrent cyber/IT threat?
- Have emergency response plans been exercised for security-based events?
  - Nuclear Energy Institute (NEI) has developed some guidance (NEI 06-04)

Relatively large publication bases

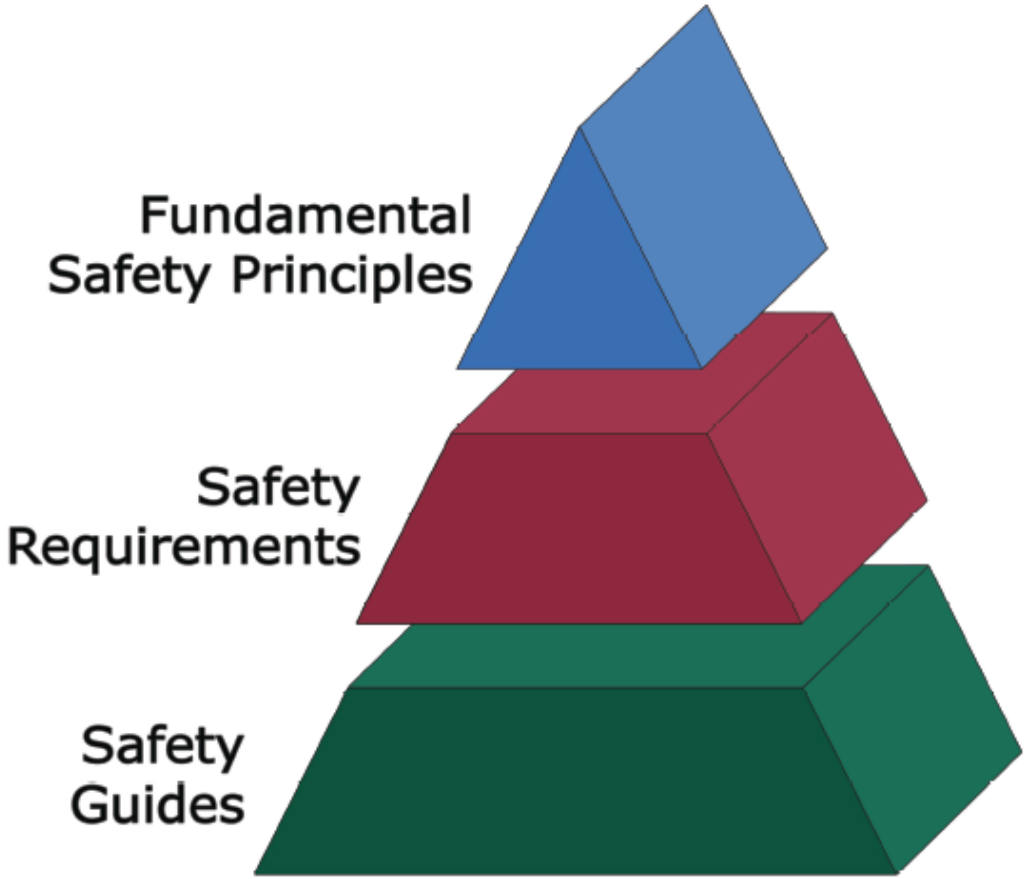




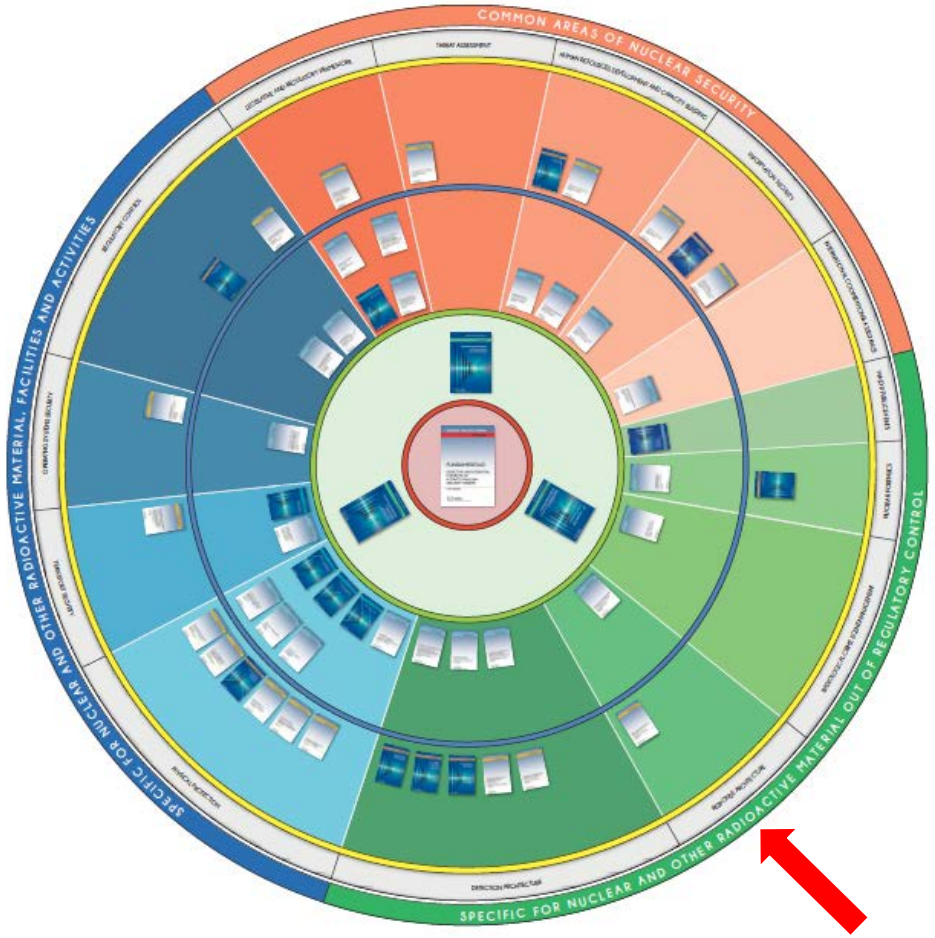
Nuclear Safety Series



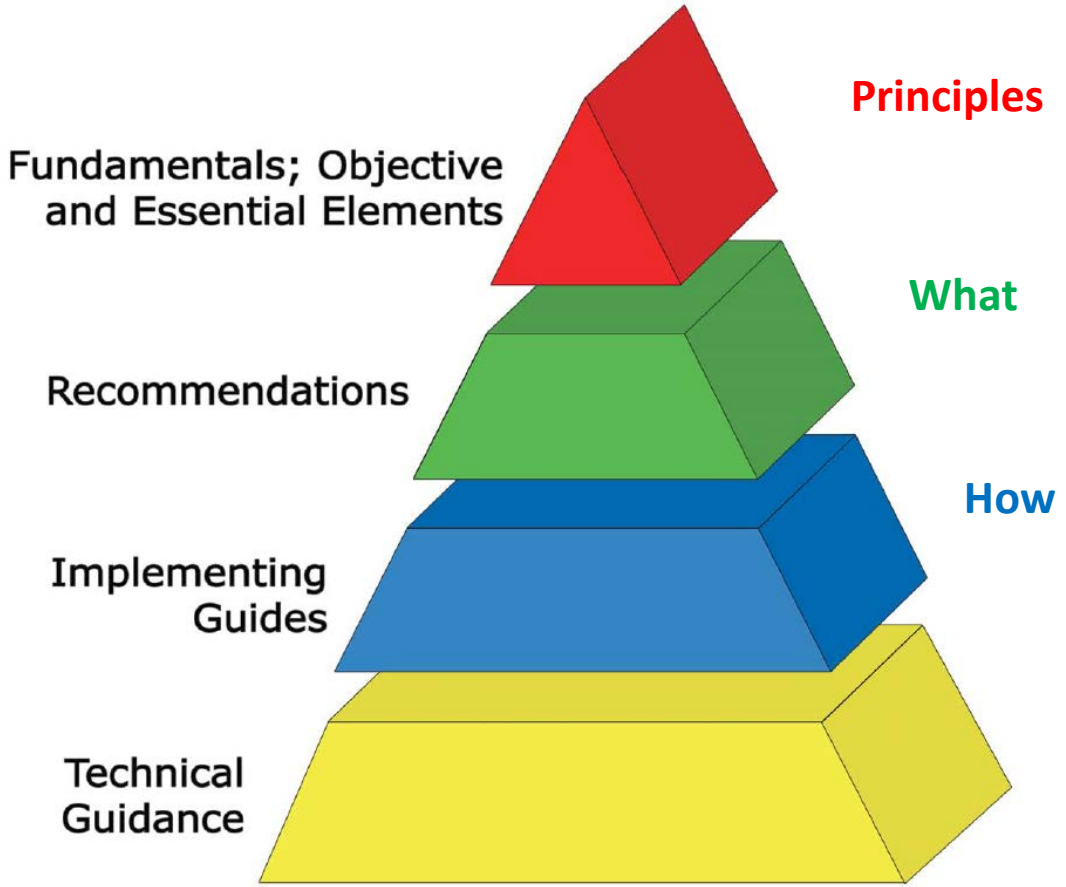
Response

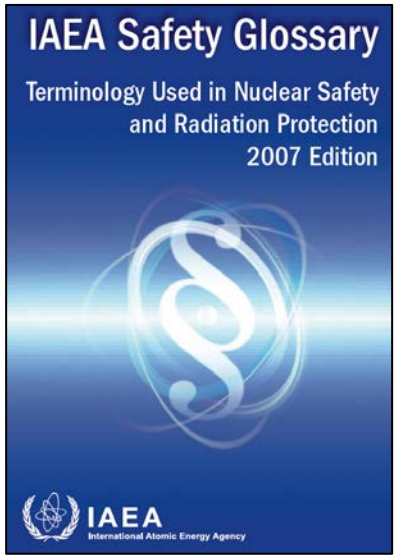


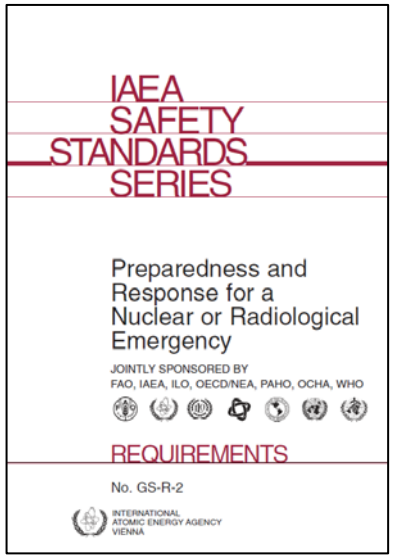
Nuclear Security Series

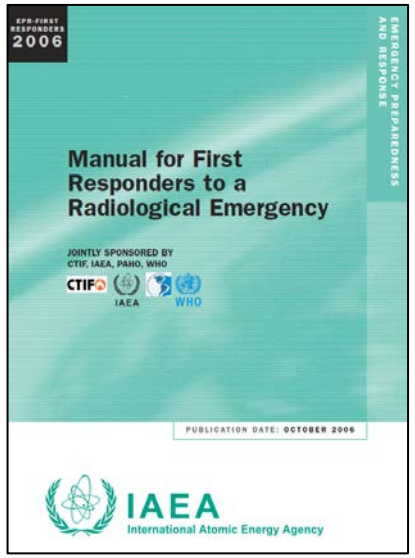


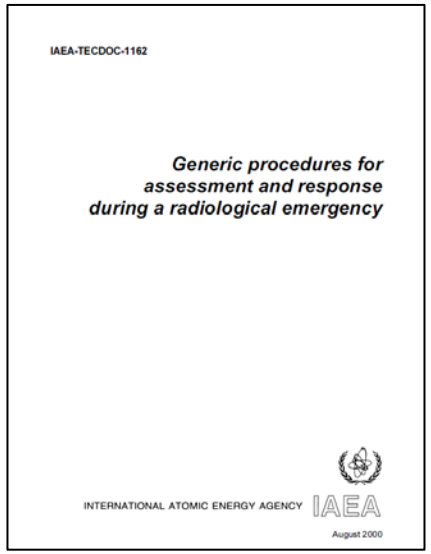
Response

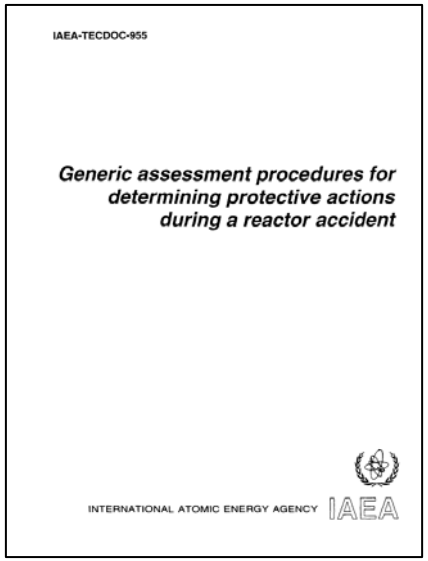


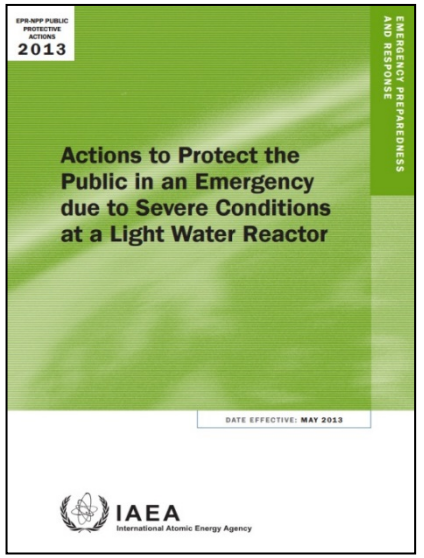


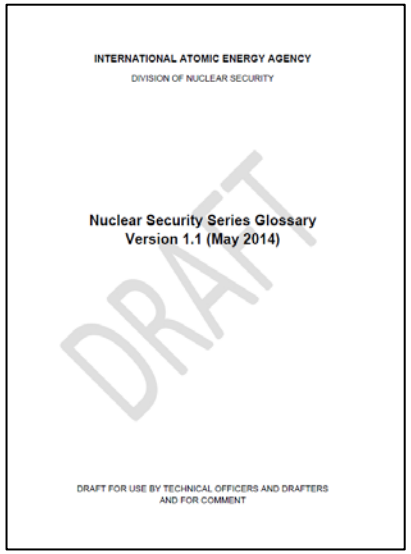












Malicious acts are discussed here

Implementing and Technical Guidance documents for contingency response are planned

Conclusions

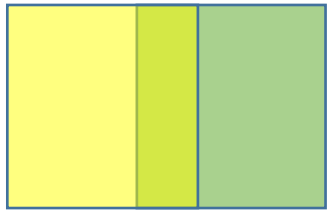
- The gap has been closing between the safety and security cultures
  - We can do better
- Assessment for emergency response is different for the safety and security organizations
  - The goal is the same
- There have been a variety of emergency response exercises that have involved security events
  - Transparency and sharing of OpEx is not as complete as with safety

Recommendations

1. Completion of the **Nuclear Security Series Glossary**
2. Development of **security response guidance**, similar to and consistent with IAEA Emergency Preparedness and Response guidance
   - Planning and Preparedness for Response to Nuclear Security Events – Implementing Guide
   - Recovery of Radioactive Material Out of Regulatory Control – Technical Guidance
3. Development of guidance for implementing a **coordinated response mechanism**
4. Development of coordinated **drill and exercise guidance** for coupled safety & security events
5. Development of guidance for fostering **synergy** of contingency (security) plans and emergency (safety) plans

Recommendations (cont)

6. Continued promotion of:
   - **Cross functional communications**: Need to know versus need to share
   - **Security Liaisons** (from safety departments)
   - **Security-informed Safety Management**: safety personnel given specialized training in nuclear security
   - **Human reliability**: establishment of high standards of individual integrity in personnel performing duties associated with the nuclear assets being protected
   - Exercising the **insider threat**
   - Exercising **IT/cybersecurity** events
   - Security-based **event tree** development to aid security response plan development
   - Completely integrated cross-functional interoperability

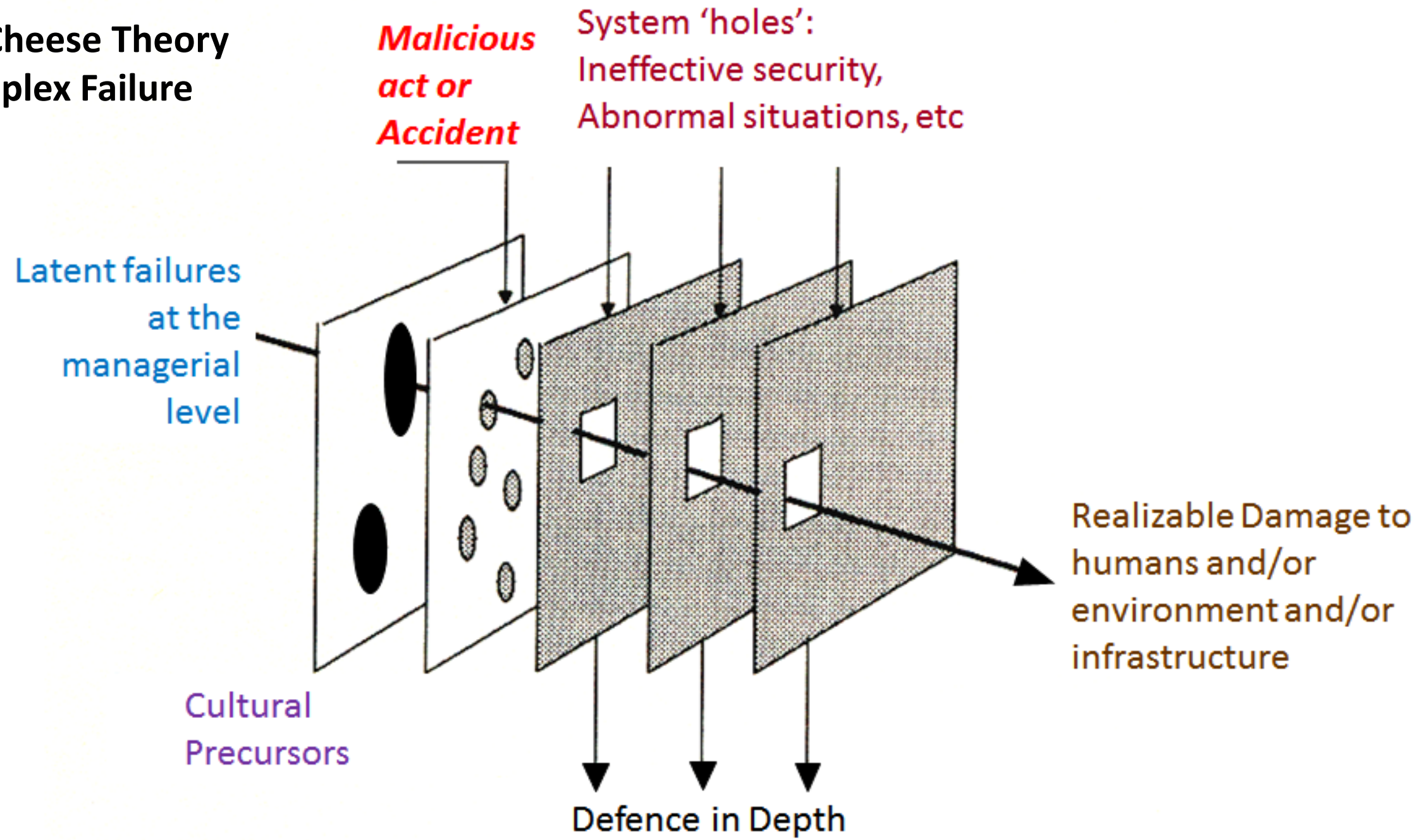


Questions?

Vision without Execution is Hallucination

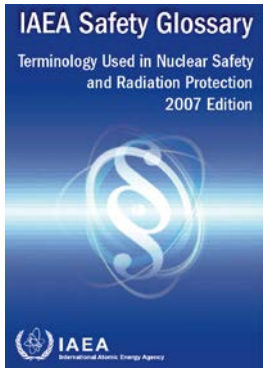
Thomas Edison

Swiss Cheese Theory of Complex Failure



Adapted from "Human Error", James Reason, Cambridge, 1990

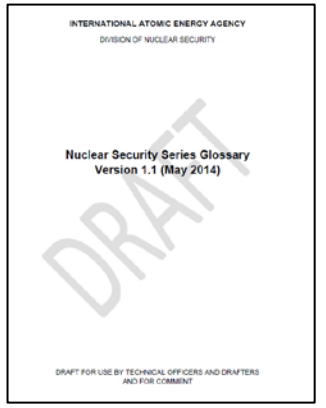
Is there consistent lingo?



- Is there a common definition of “Emergency Response”?
  - The **performance of actions to mitigate the consequences** of an *emergency* for human health and *safety*, quality of life, property and the environment. It may also provide a basis for the resumption of normal social and economic activity.
- *Emergency*:
  - A non-routine situation that necessitates prompt action, primarily to mitigate a hazard or adverse consequences for human health and *safety*, quality of life, property or the environment. This includes *nuclear and radiological emergencies* and conventional *emergencies* such as fires, release of hazardous chemicals, storms or earthquakes. It includes situations for which prompt action is warranted to mitigate the effects of a perceived hazard.

Similarly defined in EU Council Directive 2013/59/EURATOM

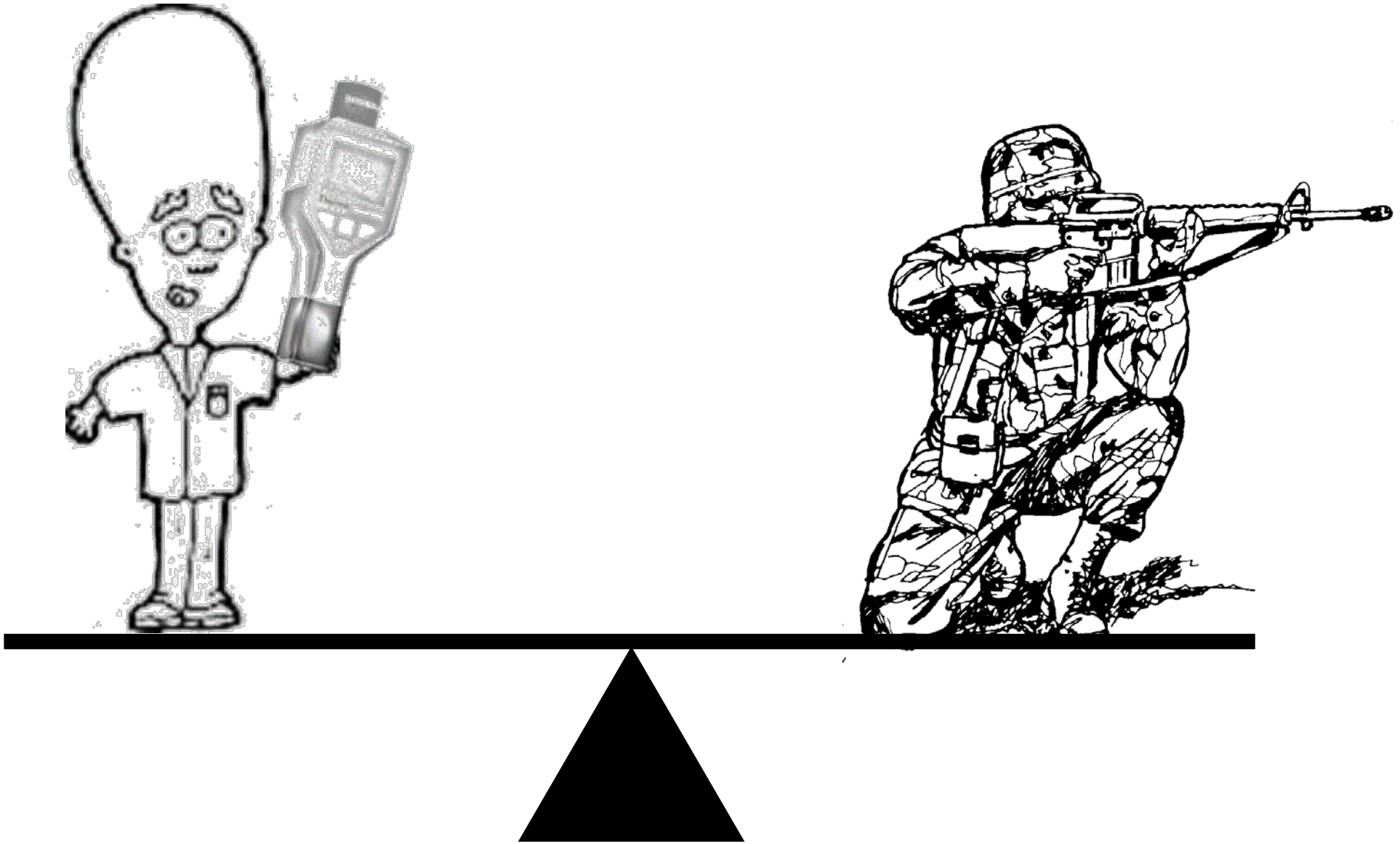
Is there consistent lingo? (cont)



- 'Emergency' and 'Emergency Response' are not defined in the DRAFT Nuclear Security Glossary. **Response** is defined as
  - All of the activities by a State that involve assessing and responding to a *nuclear security event*
  - In safety, "response" normally refers to response to a nuclear or radiological emergency, i.e. to the consequences for the safety of people and the environment of an accident or a *nuclear security event*. **In security, "response" normally refers to response to a *nuclear security event* itself, including identifying, pursuing and interdicting the cause of the event.**

- Safety is about protecting humans from radioactive sources
- Security is about protecting radioactive sources from humans

- A security incident can rapidly turn into a safety disaster



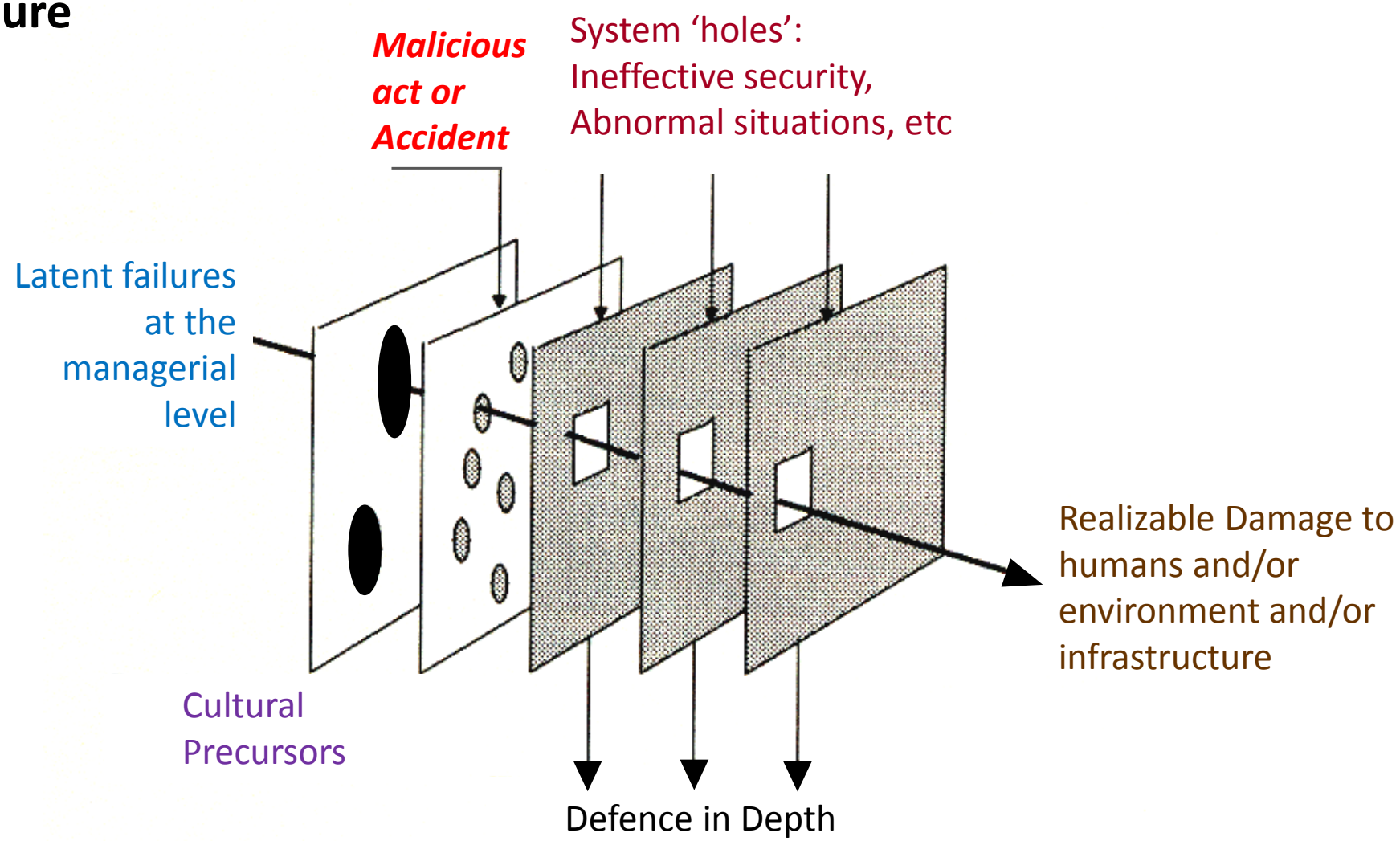
Scenario: Sabotage

- Event(s) occur to push reactor operation towards unstable operating condition, with potential for release
- (Concurrent) cyber/IT attack on reactor primary shutdown system (SDS-1)

- Are security personnel needed at the points of event initiation or SDS-1?

- Send security responders to SDS-2 overrides, which are isolated from SDS-1. This is where an attack will occur.

Swiss Cheese Theory of Complex Failure



Adapted from "Human Error", James Reason, Cambridge, 1990