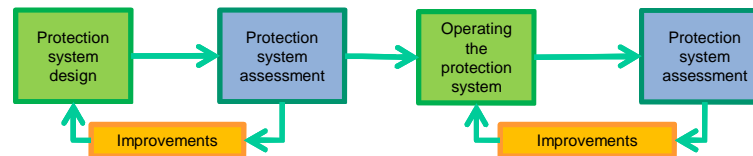


Eric GOSSET



# The assessment of the physical protection system of a nuclear facility

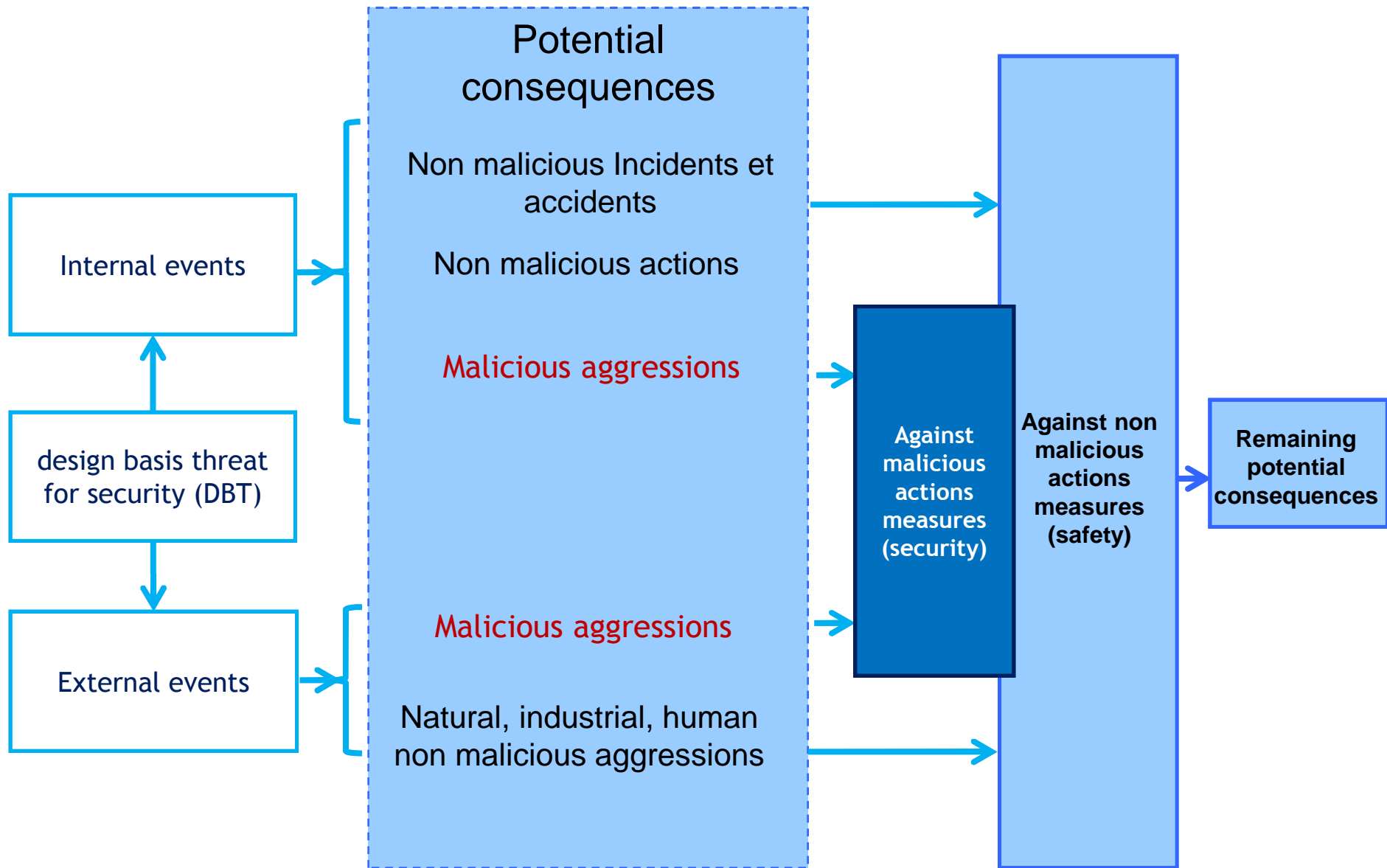
(based on the security study and the crisis management process)



# Summary

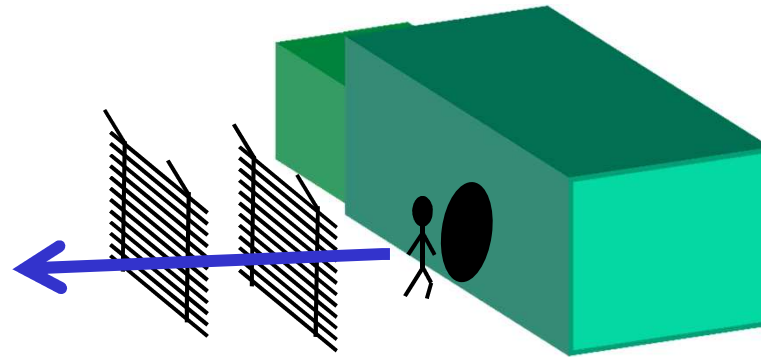
- Global potential consequences approach
- Against theft and sabotage : avoid consequences
- Connection between consequences and protection measures  
→ Protection system
- Protection system (facility) lifecycle
- Protection system design/evaluation through protection assessment studies
- Output of the protection system assessment studies
- Protection system assessment studies as part of the Authority licensing process
- Link with Emergency organization and planning

# Global potential consequences approach



# Against theft and sabotage → avoid consequences

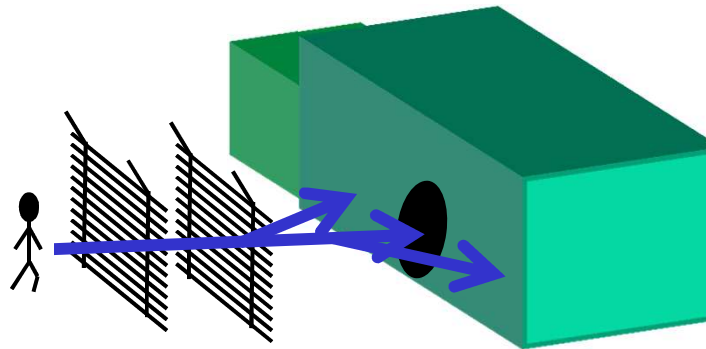
Theft or diversion: avoid nuclear material to leave the site



Response from the state  
(might be off site)

➔ Mainly a nuclear material management, physical protection & security concern

Sabotage : stop the aggression before radiological consequences are unavoidable

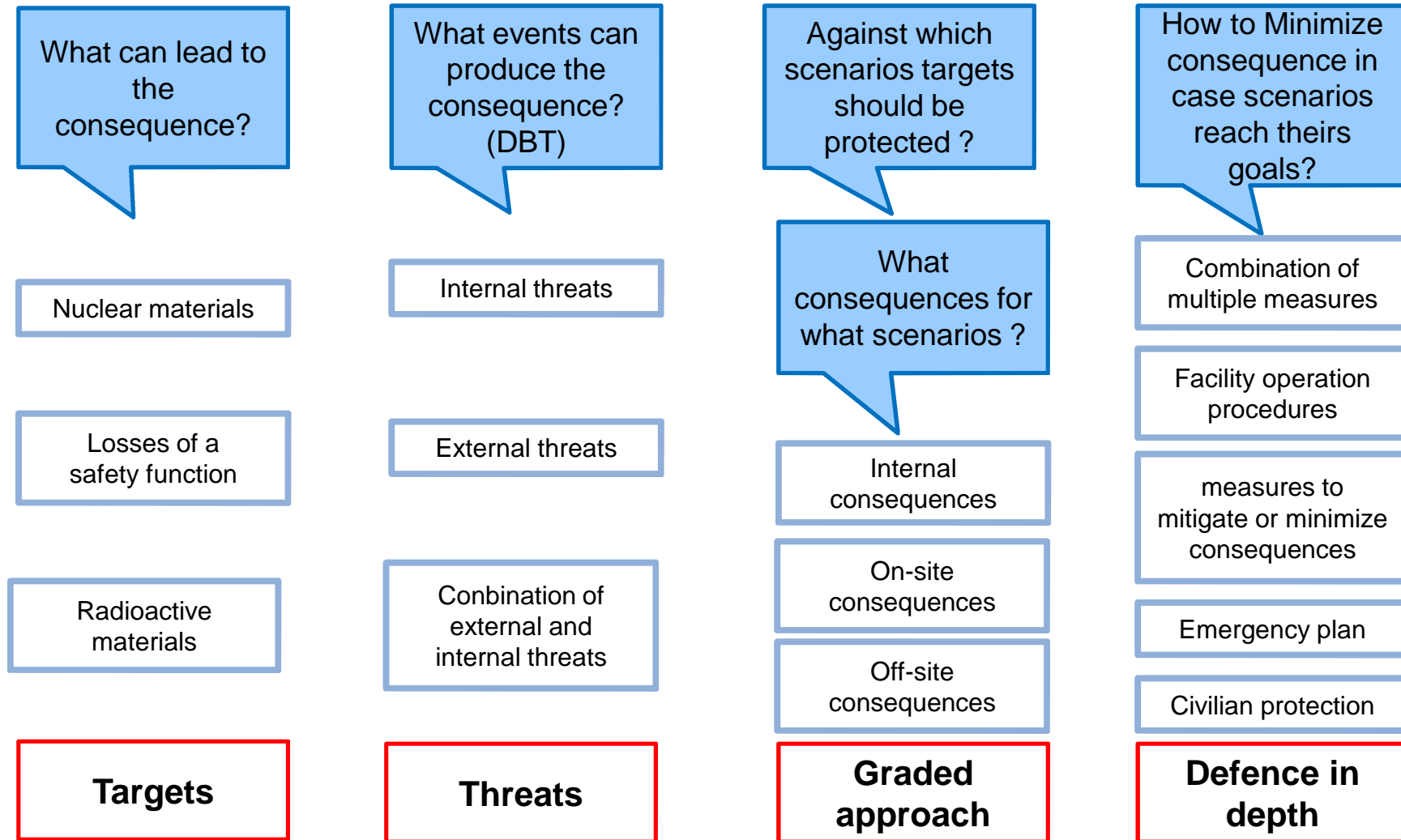


Stop adversaries by an on-site response  
On/off site State response

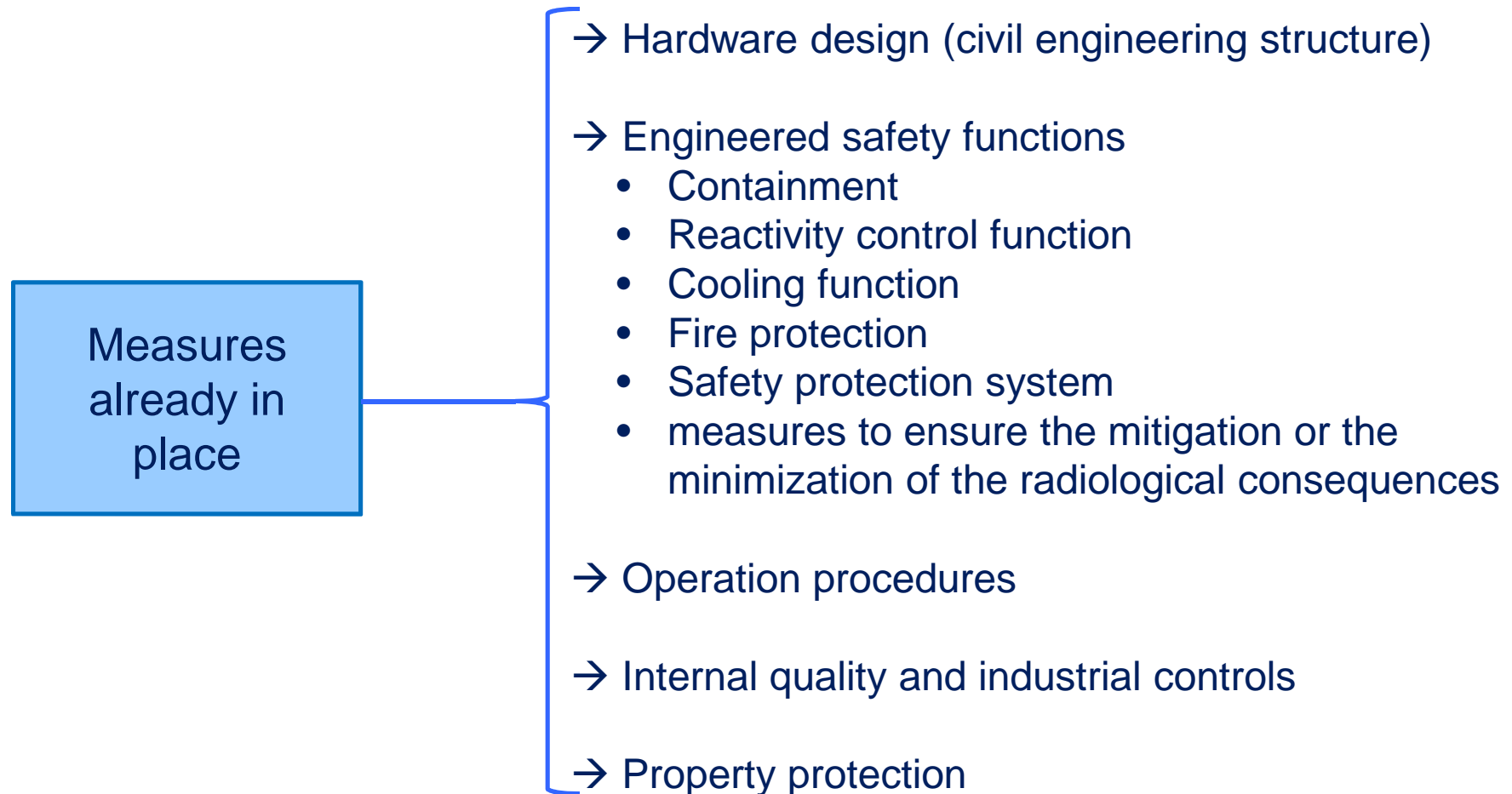
Minimize consequences  
Emergency management  
Return to a safe and secure state

➔ A combine safety, physical protection, nuclear material management & security concern

# Connection between consequences and protection measures → Protection system







## Adding existing measures with protection measures



➤ Do those measures have any sense in front of a malicious and determined attacker?

# Against which threat : internal, external, trained, equipped, having information ?

→ Protection measures have to be effective against the threat

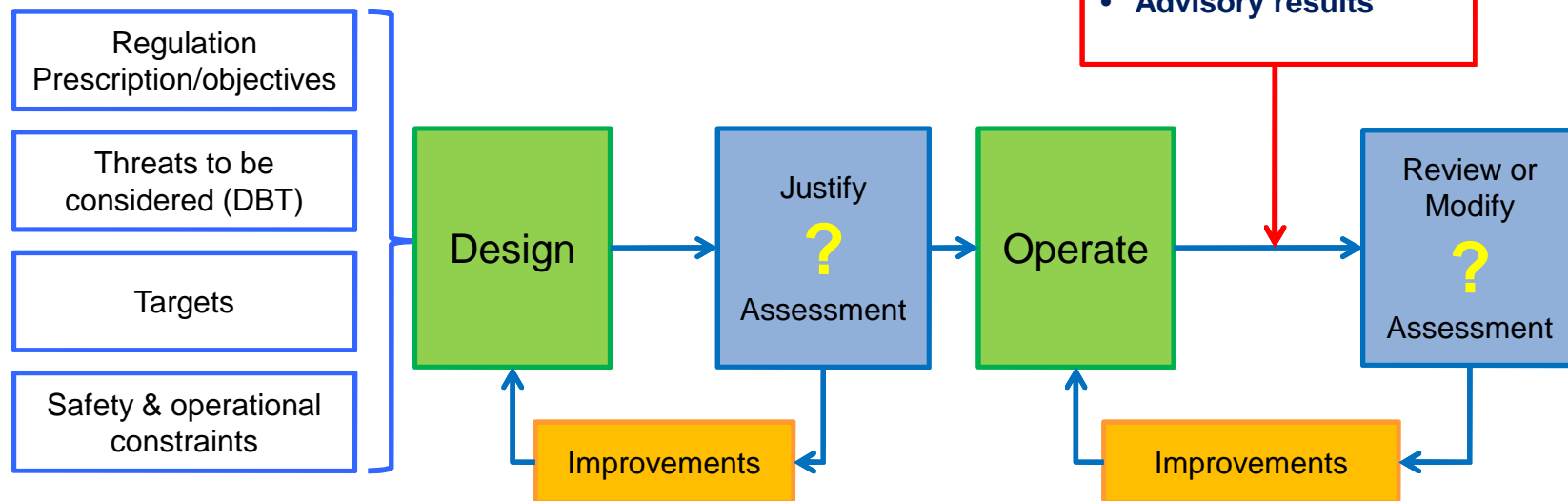
<p><b>Deter</b></p> 	<p><b>Detect to respond</b></p> 	<p><b>Delay (slow aggression) compatible with response</b> Static or activated in case of attack</p> 	<p><b>Internal and external response force</b></p> 
---	---	--	---

**An organisation : procedures, awareness , training, tests and maintenance...**  
Nuclear material movement are under control, detection system is activated and operational, its performances are in compliance with the expected performance determined during the design

**Confidentiality**  
Target vulnerability are kept secret  
Protection measures are not public and their potential failure or weakness neither

# Protection system (facility) lifecycle

- Physical protection system assessment is required when :
  - Designing → to put the right measures in place
  - Justifying → to give guaranty to the Authority
  - Modifying → to guaranty the performance
  - Reviewing on a regular basis → sustainability



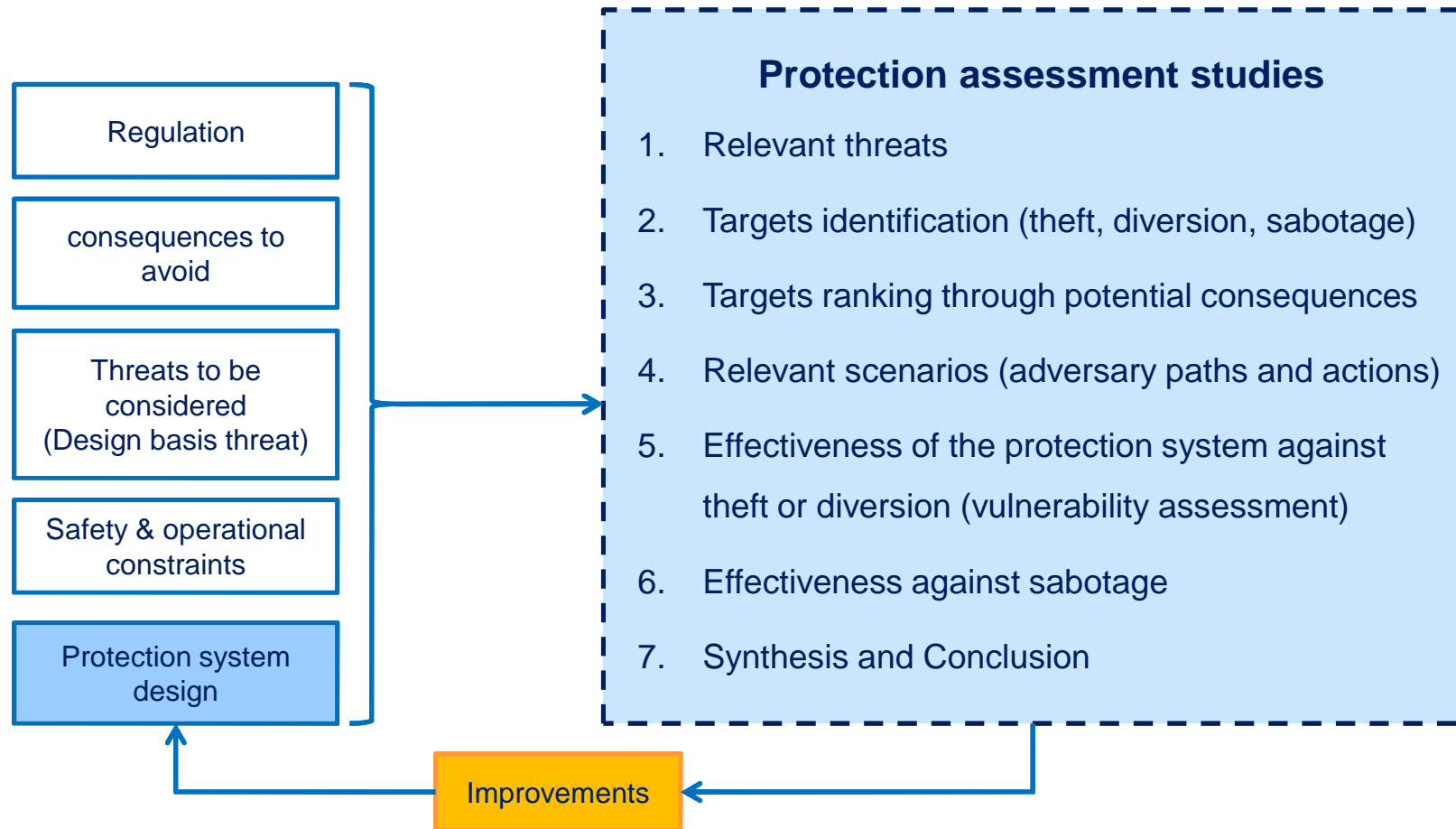


# Protection system design/evaluation through vulnerability assessment : hypothesis

- Deterministic approach
- Relevant threats
  - Identifying relevant threats allows to determine which « means » of aggression the adversaries will add to the one already in the installation
- Each facility operational state should be considered
- Taking/or not credit to accident management recovery actions and/or emergency preparedness

→ If recovery actions are considered, the ability to realise those recovery actions in presence of aggressors or after a sabotage acts has to be assessed

# Protection system design/evaluation through protection assessment studies : steps

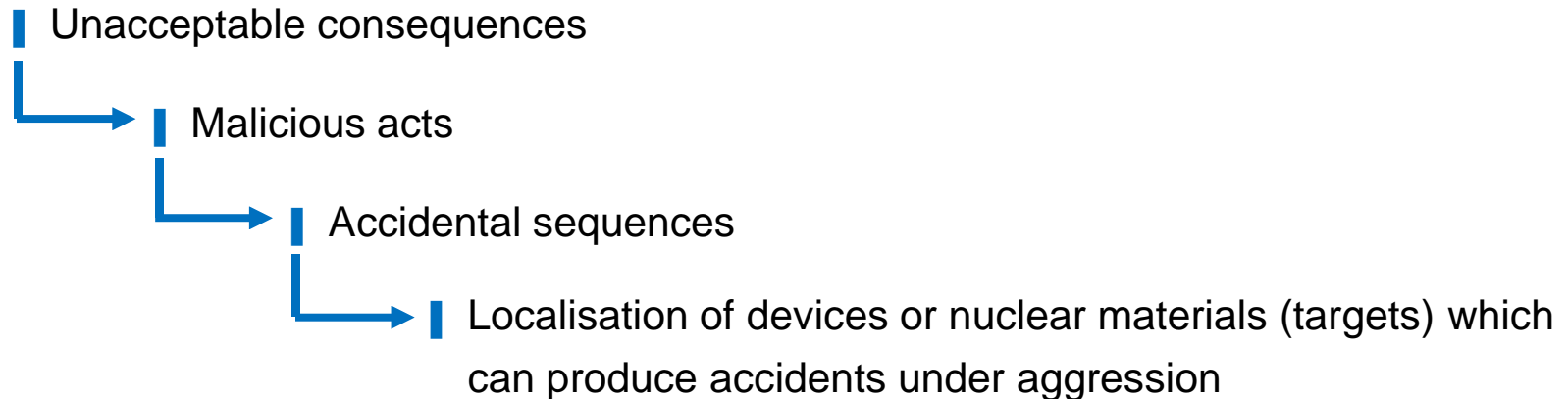


# Why a method ? and Which method ?

- Define one or more methods to :
  - Identify rigorously targets for each state of the facility
  - Define useful and coherent measures
  - Trace studied cases (to allow regular review)
  - Trace none studied cases (ones judged irrelevant)

Method for external aggression	Method for intrusion	Method for internal threats aggression
From safety studies	From safety studies	From safety studies
geographical & environmental analysis	And from expert judgement	And from expert judgement

# From consequences to targets



## First, what can malevolent do ?

- Inventory of the aggression means :
  - External actions : weapons, actions from the environment, cyber means
  - Internal actions : take control, forced stop/star, access control, mechanical, thermic, toxic explosive means, fire...
- Inventory of aggressions means already on-site (handling machines, fuel, mechanical/thermic devices, explosive, flood)

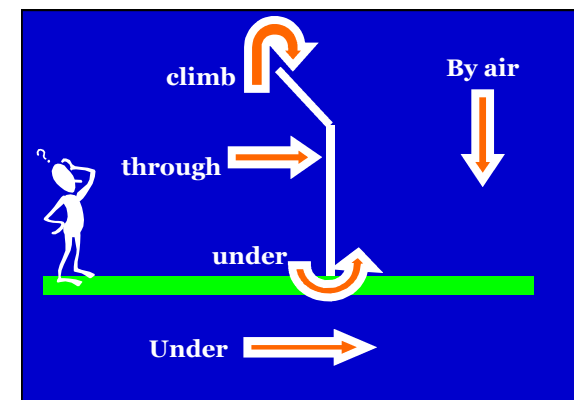
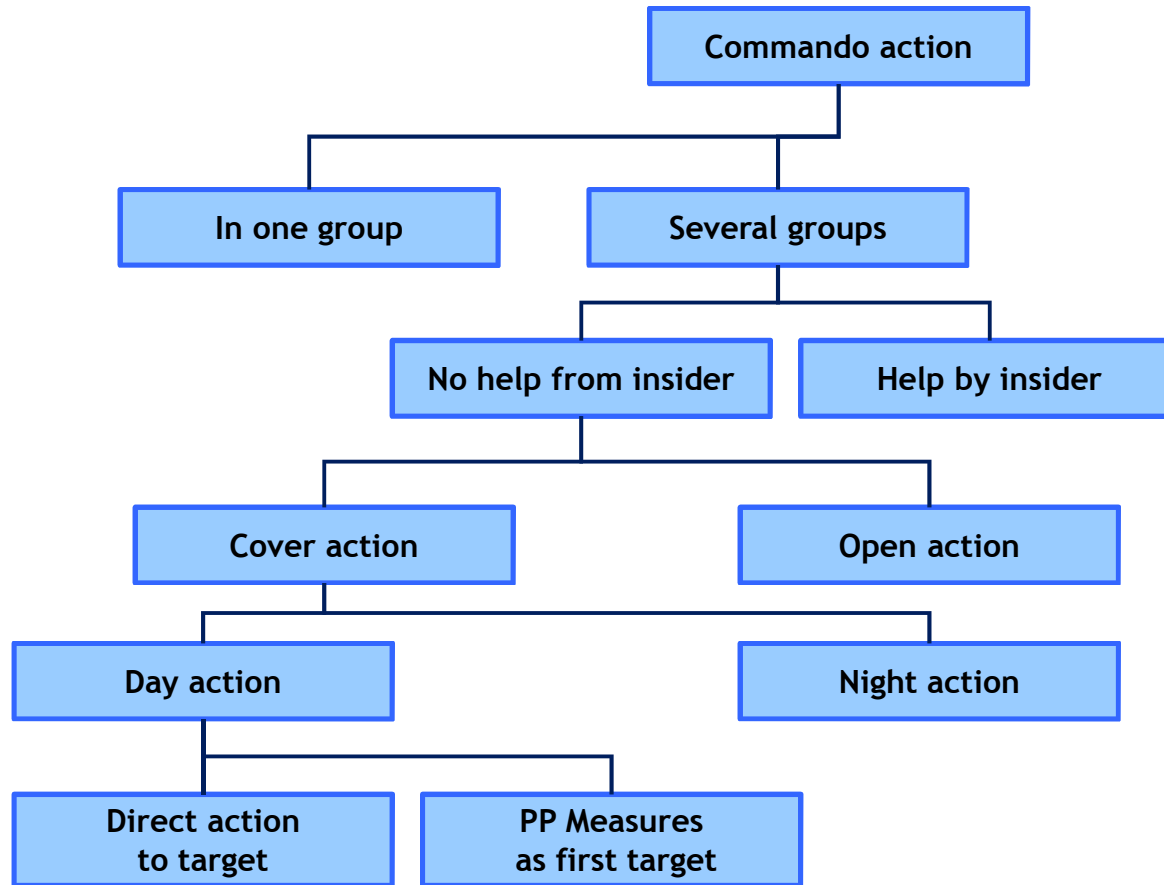
## Identify sequences of malicious actions for sabotage (accidental sequences)

- Direct sabotage of nuclear or other radioactive material inventory (with the means of the threats or present on-site)
- Indirect sabotage of nuclear or other radioactive material

Acts against systems, structures, components, equipment, devices or operator actions (SSC) that normally maintain the facility in a safe state and will lead indirectly to radioactive release higher than the defined threshold, in case of dysfunction.

- Initiating events addressed in safety analysis
- Initiating events not addressed in the safety analysis (failures excluded from consideration because they are unlikely to occur randomly)
- Events not addressed in safety analysis ? (expert judgement)
- Any event beyond the threat capabilities can be eliminated
- Functional studies have to be complemented by a geographic approach as the aggression is made by individuals
- Collateral damages have to be identify

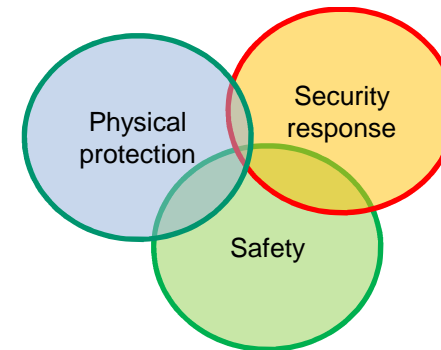
# Adversary actions and path



# Vulnerability assessment and system response

- Each relevant scenario is evaluate taking into account ALL protection measures :

- Facility design (robustness)
- Safety (redundancy, fire protection)
- Radiation protection (biological protection)
- Physical protection (detection, alert, delay)
- Response (response forces, provisions dynamic)
- mitigation systems (fixed or dynamic if they are realistic in the context of threat)
- Repair actions to return to stable (if they are realistic in the context of threat)



➔ Identify possible final state of the facility (both for safety and security), determined potential consequences

➔ Involve Safety, physical protection, security specialists

➔ Emergency management organisation should be included

# Output of protection assessment studies

**Complementary to measures prescribed in regulation  
Protection system is adapted to each facility**

Target ranking through potential consequences for graded approach

Weakest points to be protected in reflex mode (strategy)

Effectiveness and coherence of protection measures

Potential facility states after attack

Feasibility of repair actions

**Gives inputs for emergency planning**



# Protection system assessment studies as part of the Authority licensing process

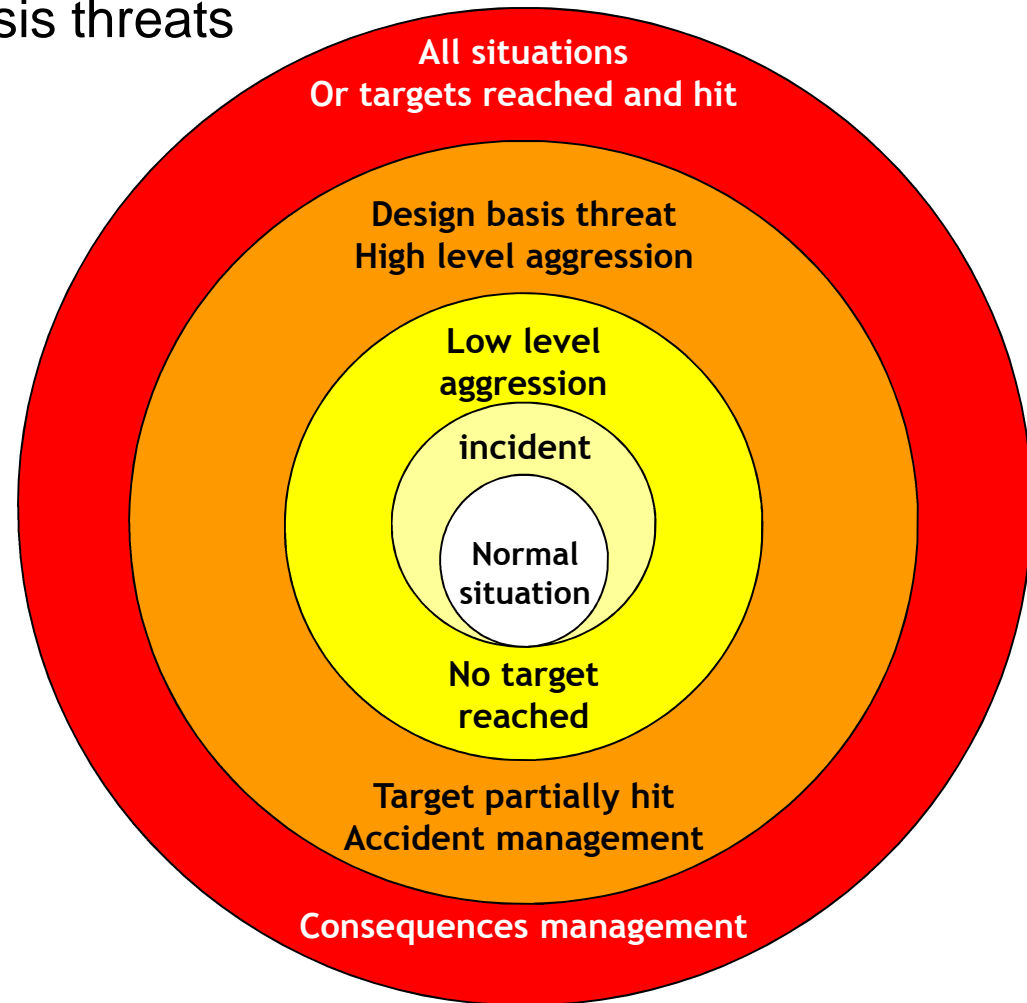
- ACCEPTANCE REST ON COMPETENT AUTHORITIES
  - Considering the regulation prescription
  - Considering the design basis threat (DBT)
  - Considering the comparison between results of the protection system assessment and the protection objectives
  - Considering the response forces capabilities
  - Considering emergency plans
  - Considering potential off-site consequences
  - Considering State policy
  - Considering the cost/benefit of measures to be taken
  - Considering the technical support body evaluation of the assessment
  - ...

## Links with emergency organisation and planning

- Protection assessment studies are justifying the efficiency of the protection system facing the design basis threats

- Emergency organisation should be able to face all situations !

→ **Defence in depth**



# In conclusion

## Complex studies but many valuable outputs

Enhanced perception of the risk

Safety, security, physical protection specialists sharing knowledge

Development of security culture

Repair strategy in conjunction with safe restoration action

Conduct procedure of a facility under attack

Coherence with emergency planning