CESI RICERCA

DAMSE

EC funded project
JLS/2006/EPCIP/001

CESI RICERCA · MINISTERIO DE MEDIO AMBIENTE · CONFEDERACIÓN HIDROGRÁFICA DEL JÚCAR · Verbund · CVA

A European Methodology for the Security Assessment of Dams

Project Summary

by Massimo Meghella, CESI RICERCA Spa

Final meeting, Valencia, February, 25th-26th, 2008

Objectives

The project is aimed at the development and the verification of a methodology for the ***security assessment*** of dams against threats such as: ***terrorist attacks, sabotage*** and ***malevolent intrusions***.

*(*to be proposed as a common framework for the effective protection of dams at EU level).

Motivation for funding by EC

- ✓ recognition that ***protection*** of dams against natural hazard and terrorist attack/sabotage is nowadays a ***hot critical*** issue in European countries, considering that dams are a vital part of ***Europe infrastructures***;

- ✓ lack of systematic and rational approaches for the ***security assessment and management of dams***, either at national and European level;

Motivation for funding by EC

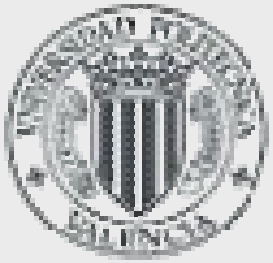
- ✓ lack of technical and decisional tools to support ***risk mapping*** of dams, with regards to terrorist threats at European level;

- ✓ trans-national nature of the project (3 important European countries, ***Austria***, ***Italy*** and ***Spain***, with more than 30% of all EU large dams, are represented)

Main figures

- ***Duration***: 1 year (from 31/12/2006) + 2 months extention
- ***Partners***: 2 developers

CESI RICERCA



3 end-users

Verbund

MINISTERIO DE MEDIO AMBIENTE
CONFEDERACIÓN HIDROGRÁFICA DEL JÚCAR

CVA

- ***Budget***: 231,903 €
- ***Funding from EC***: 197,118 € (85%)

Main components

- ✓ a ***threat assessment*** procedure for the determination of the likelihood of malevolent adversary attacks, sabotages and intrusions to a critical asset;
- ✓ a procedure for the ***consequence assessment*** in case the threats would succeed in compromising the ability of the dam to accomplish its mission
- ✓ a procedure for determining the ***effectiveness*** of the security protection system to prevent an attack against an operational component or a critical asset of the dam

Main components

- ✓ a ***risk assessment*** procedure to support managers to evaluate the level of risk associated with the threat, consequences, and protective system effectiveness and to identify the needs in terms of ***security upgrades*** or consequence mitigation for ***risk reduction***;

- ✓ a ***survey*** procedure aimed at ***verifying*** the development of the methodology and at ***demonstrating*** the above procedures on a set of dams, identified following a screening among the ***dam portfolios*** provided by partners;

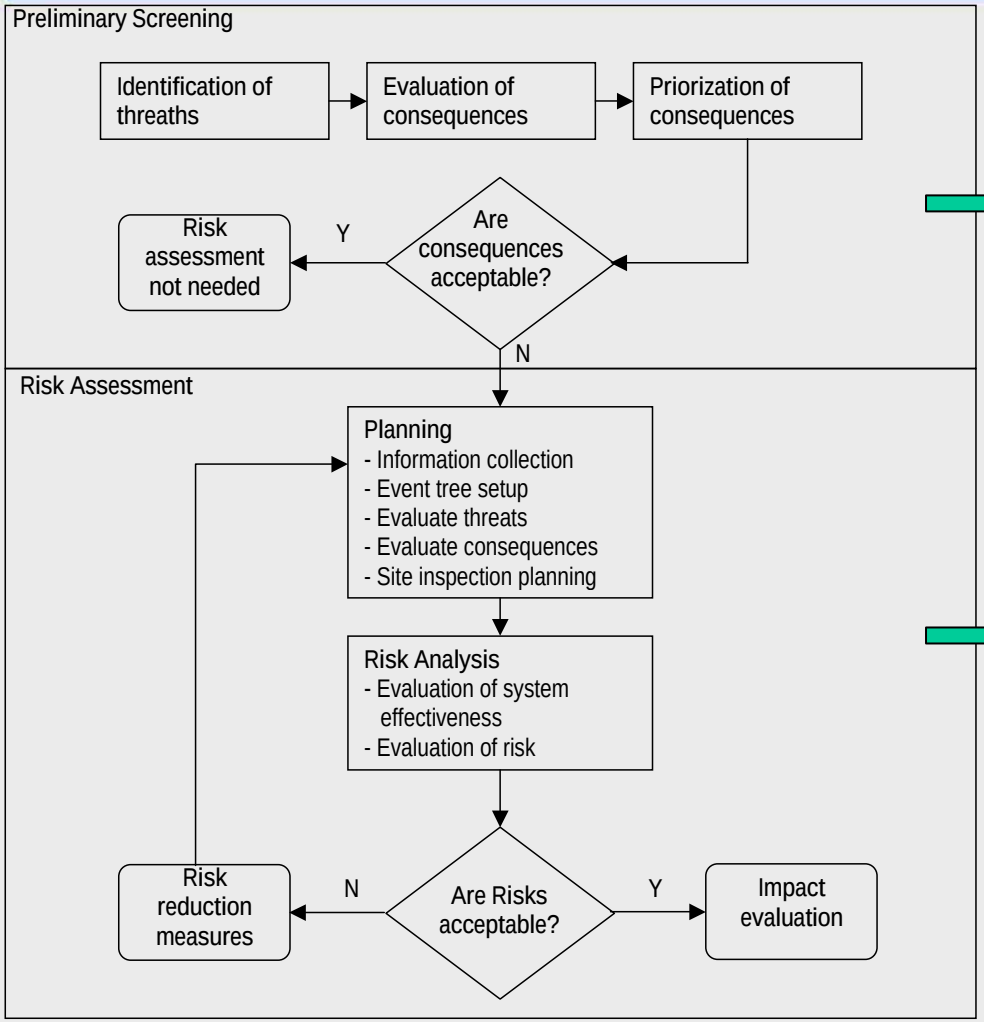
Approach

- ✓ ***Developer partners*** (CESI RIC and UPV) to develop the methodology and to facilitate its correct application
- ✓ ***End-users partners*** (Verbund, CVA, JUCAR) to provide the input and know-how to customize the methodology to their specific needs and to verify the methodology on their dams portfolios

Approach

- ✓ An ***expert panel***, composed of qualified international experts in dam engineering and risk analysis, to review and to evaluate the project results
- ✓ A suitable ***confidentiality policy*** to prevent intentional and malevolent access and disclosure of sensitive data and information related to safety and security

Methodology



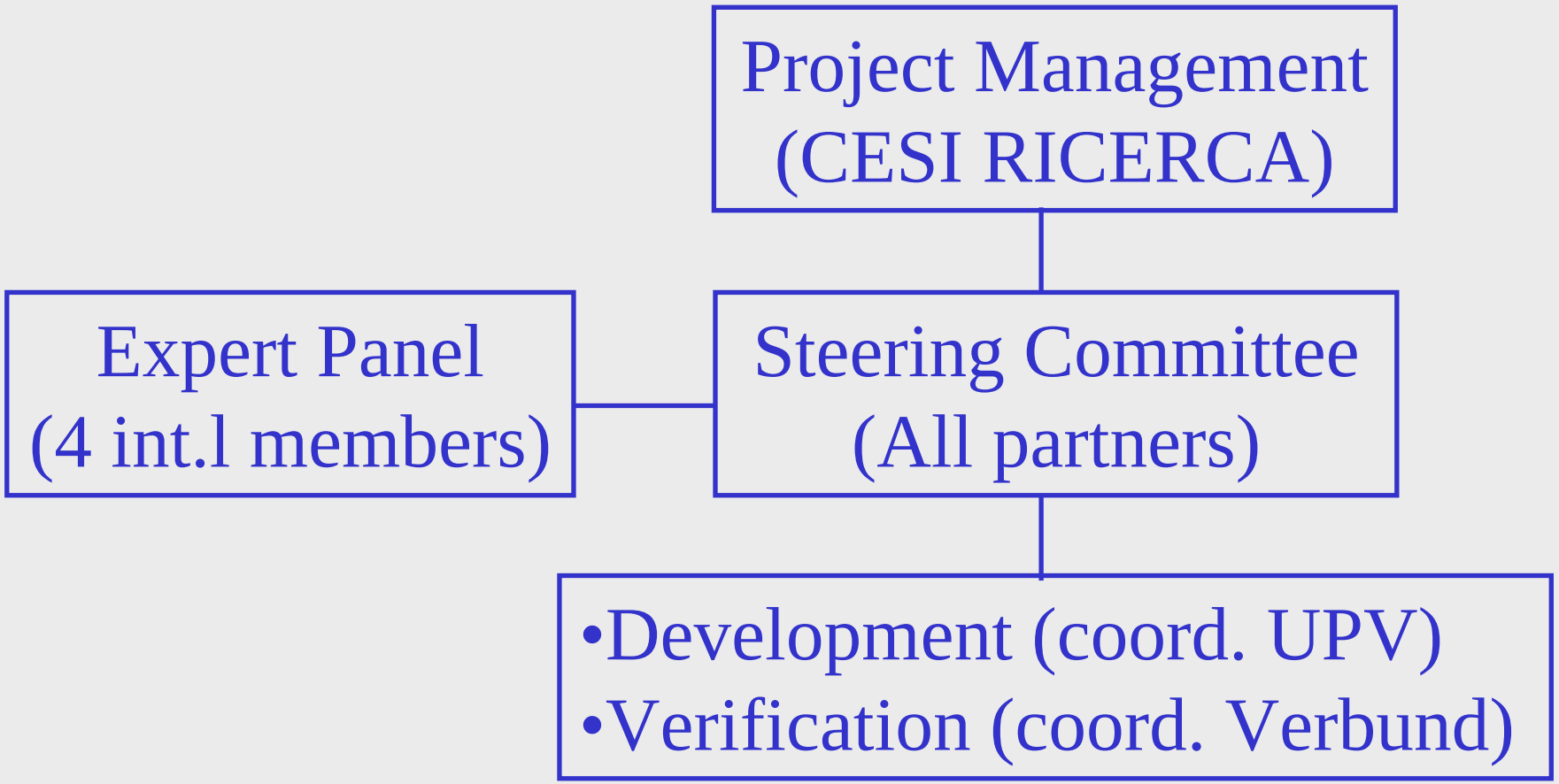
3 most critical dams for each end-user

Security Fault Tree

$$Risk = R(L, V, C)$$

L = Likel. of Attack
V = System Inadeq.
C = Consequences

Organization & Implementation



Work Plan

	MONTHS												man
Activity	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**days**
Project Management	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**	**6.0**	50.0
Kick-off meeting	**10.0**												10.0
1 Selection of a dams portfolio	**10.0**												10.0
2 Development of a simplified procedure for dams screening													0.0
2.1 Identification of undesired events	**10.0**												10.0
2.2 Identification of event consequences		**10.0**											10.0
2.3 Definition of criteria for avoiding a full risk assessment analysis		**10.0**											10.0
2.4 Procedure implementation in work-sheets	**15.0**	**15.0**											30.0
3 Screening of all the dams in the end-user portfolio			**10.0**	**20.0**	**20.0**								50.0
Intermediate meeting to discuss Expert Panel evaluation of results							**10.0**						10.0
4 Development of a full risk assessment procedure													0.0
4.1 Identification of site information need			**10.0**										10.0
4.2 Development of a Security Dam Fault Tree			**20.0**										20.0
4.3 Identification of adversaries and attack scenarios				**20.0**									20.0
4.4 Determination of event consequencies in detail					**10.0**								10.0
4.5 Definition of site survey planning					**20.0**								20.0
4.6 Development of a system effectiveness procedure						**10.0**							10.0
4.7 Development of a risk analysis procedure						**20.0**							20.0
4.8 Guide in the selection of security system upgrading for risk reduction							**20.0**						20.0
4.7 Development of a procedure for upgrading impact evaluation							**20.0**						20.0
													0.0
5 Full risk assessment of a sub set of end-user dam portfolio								**20.0**	**20.0**	**20.0**	**20.0**	**20.0**	100.0
Complete evaluation of the project during the final Expert Panel meeting												**10.0**	10.0
Final report												**X**	0.0
	49.0	39.0	44.0	44.0	54.0	34.0	54.0	24.0	24.0	24.0	24.0	36.0	**450**

Meetings

- ✓ ***Kick-off,*** ***Vienna, 15-16 Feb. 2007***
- ✓ ***Mid-term,*** ***Milan, 2-3 Aug. 2007***
- ✓ ***Final,*** ***Valencia, 25-26 Feb. 2008***

Final Event

- ✓ ***Workshop, Valencia (26 Feb. 2008)***

  (With expert panel members. Dissemination of results among dam engineering community, dam operators, public authorities, civil protection, etc.)

Dam Survays

Dams identified following the preliminary screening procedure. :

- ✓ ***3 CVA dams*** ***(Sep. 2007)***
- ✓ ***3 Verbund dams*** ***(Oct. 2007)***
- ✓ ***3 Jucar dams*** ***(Nov. 2007)***

Consortium Agreement

The **Consortium Agreement** addresses the following issues:

- ***Property rights:*** jointly shared between developers (CESI RIC. and UPV)
- ***License rights:*** Permanent license rights to all end-users (Verbund, CVA, Jucar)
- ***Confidentiality policy:*** Consortium vs. public and third parties; Consortium vs. EC; Developers vs. End-users; Consortium vs. Expert panel members

Expert Panel

The external review by EP (composed by ***4 international experts*** appointed by CESI RICERCA, upon acceptance of the confidentiality policy):

- ✓ to *review* the methodology according to the workplan;
- ✓ to *assess* quality and innovation of results;
- ✓ to *identify* limitations and further improvements

Expert Panel

The EP members :

- ✓ ***David Bowles,*** USA (Professor at Utah State University, Risk Analysis/Assessment/Management, dam engineering and safety assessment)
- ✓ ***Robin Charlwood***, USA (Consultant, Dam engineering and safety assessment)
- ✓ ***Rudy Matalucci***, USA (Consultant, Civil Engineering, Risk assessment and security technology)
- ✓ ***Enrique Matheu***, USA (DHS officer, Risk Analysis/Assessment/Management, dam engineering and safety assessment

Background

In Italy the public funded ***Research Programme for the Electric System (RdS)*** has recognized the need to ***identify***, ***assess***, and ***control*** risks associated with the ***security*** of its critical infrastructure assets, including ***power grid*** and ***dams***, considering that demands on the services provided by these facilities are increasing, and the condition of the assets is deteriorating, as they are nearing or surpassing their design life.

Background

RdS activities in 2006 (by CESI RICERCA with contributions from R. Charlwood, R. Matalucci and CVA):

- ✓ ***Review*** of security risk assessment methodologies, singling out those more applicable to ***dams*** and ***electric transmission grids***;
- ✓ Individuation of ***security requirements*** for Italian dams and electric transmission grids based on a trial application of DAMS-VR to CVA dams;
- ✓ Proposal for a ***road map*** to facilitate the development, verification, demonstration and acceptance of a security risk assessment methodology in the Italian context.

Background

As a response to a Presidential Decision Directives 62 (***Combating Terrorism***) and 63 (***Critical Infrastructure Protection***), the ***Interagency Forum for Infrastructure Protection (IFIP)*** was chartered in 1997 as a forum for exchange of security and protection system information among owners and operators of federal dams and related infrastructure.

Background

IFIP members:

- ✓ US Army Corps of Engineers ***(USACE)***
- ✓ U.S. Bureau of Reclamation ***(USBR)***
- ✓ Tennessee Valley Authority ***(TVA)***
- ✓ Bonneville Power Administration ***(BPA)***
- ✓ Western Area Power Administration ***(WAPA)***
- ✓ Federal Bureau of Investigation ***(FBI)***
- ✓ U.S. Department of Energy ***(USDOE)***
- ✓ Sandia National Laboratories ***(SNL)***

Background

IFIP purpose:

- ✓ Risk Assessment Methodology for Dams ***(RAM-D)***
- ✓ Risk Assessment Methodology for Transmission ***(RAM-T)***

Both of these methodologies applied an existing security risk assessment process developed early for protection of the U.S. national weapons complex.

Following the development effort at SNL, the IFIP pursued a field verification process for RAM-D^{SM} at two major Federal dams owned by USBR, and USACE, respectively.

Background

Available methodology and tools:

- ✓ ***RAM-D and RAM-T*** methodologies developed by Sandia National Laboratories for dams and transmission systems;
- ✓ ***DAMSVR*** developed for FERC by William Foos & Associates for dams;
- ✓ ***MATRIX*** Security Risk Analysis Program developed by USBR for dams;
- ✓ ***CARVER***, a check list approach, and other similar systems;
- ✓ ***RAMCAP***, Risk Analysis and Management for Critical Asset Protection.

Background

Security concerns thoroughly addressed by the EC through:

- ✓ ***Justice and Freedom Department*** in 2004 launched the ***European Programme for Critical Infrastructure Protection (EPCIP)*** aimed at enhancing EU prevention, preparedness and response to terrorist attacks involving critical infrastructures;
- ✓ ***7th Research Framework Programme (FP7)*** widely supports R&D activities in the same fields.

Requirements

Essential requirements:

- ✓ ***Rigorous risk-based*** security assessment methodology
- ✓ ***Repeatability*** of results if same input data is applied;
- ✓ ***Quantified*** relative risk provided to owner;
- ✓ ***Standardized baseline*** and common risk terminology
- ✓ ***Accountability*** by the decision-makers (assumptions, decisions, acceptable risk);
- ✓ ***Traceable*** path of assessment data and risks involved;
- ✓ ***Consistent terminology*** with all associated industries involved;
- ✓ Ease in future ***automation.***

Requirements

Advantages of RAM-D:

- ✓ Can be applied in various levels of detail as determined by the needs of the project and owner/stakeholder ;
- ✓ Includes a rational basis for security risk analyses, and adequate documentation for selecting components for analysis and for identifying critical assets within a project;
- ✓ Structured documentation systems and extensive worksheets granting the repeatability requirement;

Requirements

Advantages of RAM-D:

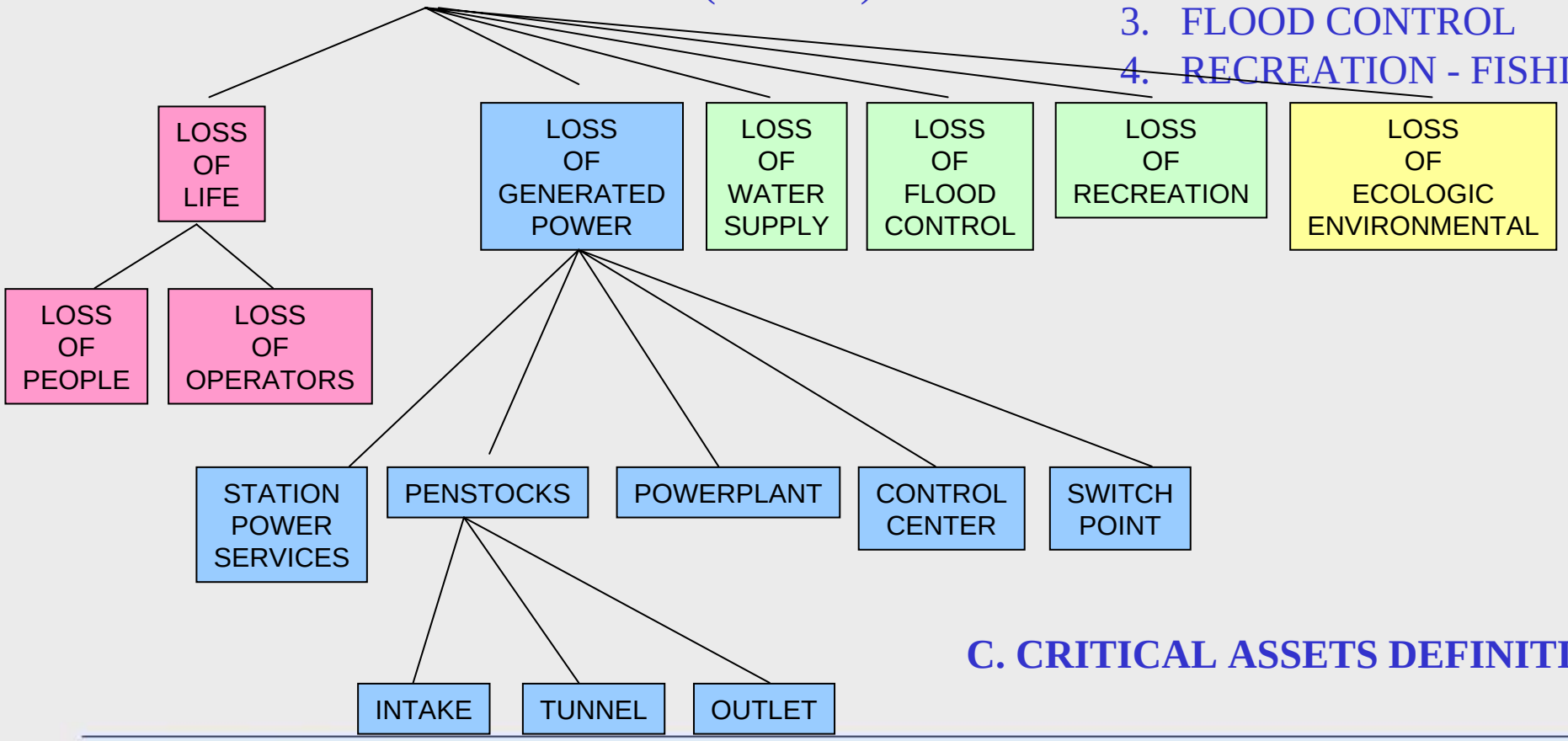
- ✓ The risk computation algorithms recognize that certain key inputs, particularly threat, cannot be defined in statistical probability terms and therefore uses a three (L, M, H) or five (VL, L, M, H, VH) level likelihood grading system to compute a relative risk number which preserves the risk logic;
- ✓ Results provide a clear basis for determining required security protective measures where their effectiveness is related to estimates of risk reduction potential;

Proposed Security Methodology

A. DAM MISSION

1. POWER GENERATION
2. WATER TO IRRIGATION
3. FLOOD CONTROL
4. RECREATION - FISHING

B. LOST OF MISSION (fault tree)



C. CRITICAL ASSETS DEFINITION

Proposed Security Methodology

D. CONSEQUENCE OF LOST MISSION (in €)
d1. loss of lifes
d2. loss of generated power
d3. loss of critical asset

E. ATTACK SCENARIO (treaths)
e1. vandals (high)
e2. criminals (high)
e3. eco-T (medium)
e4. military (medium)
e5. …
e6. Al-Qaeda (low)

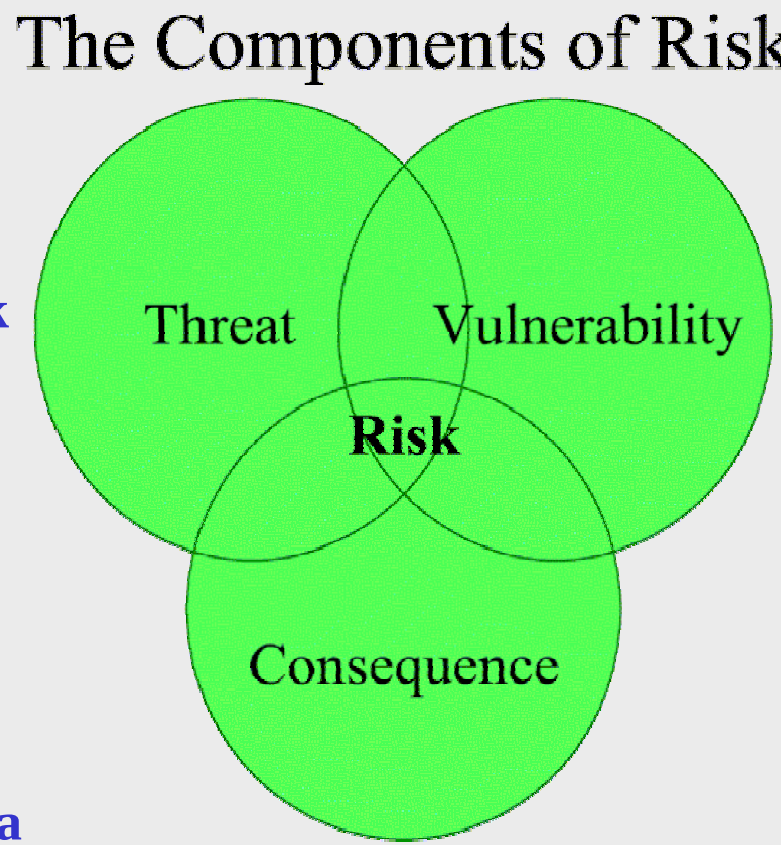
F. SECURITY STRATEGY
f1. today
f2. attack scenario considered

G. DESIGN

H. RISK REDUCTION

$$R = R(T,V,C)$$

Proposed Security Methodology

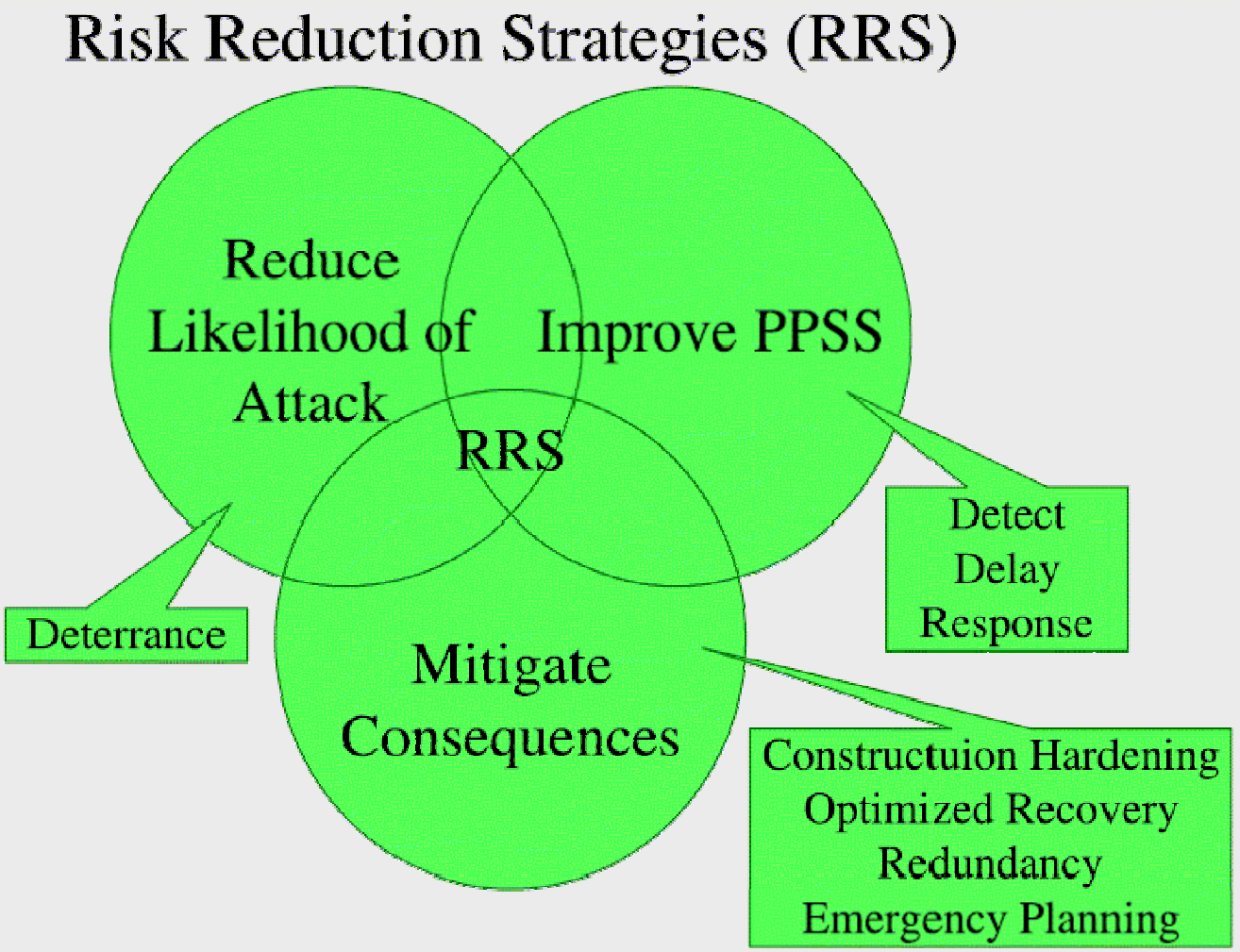


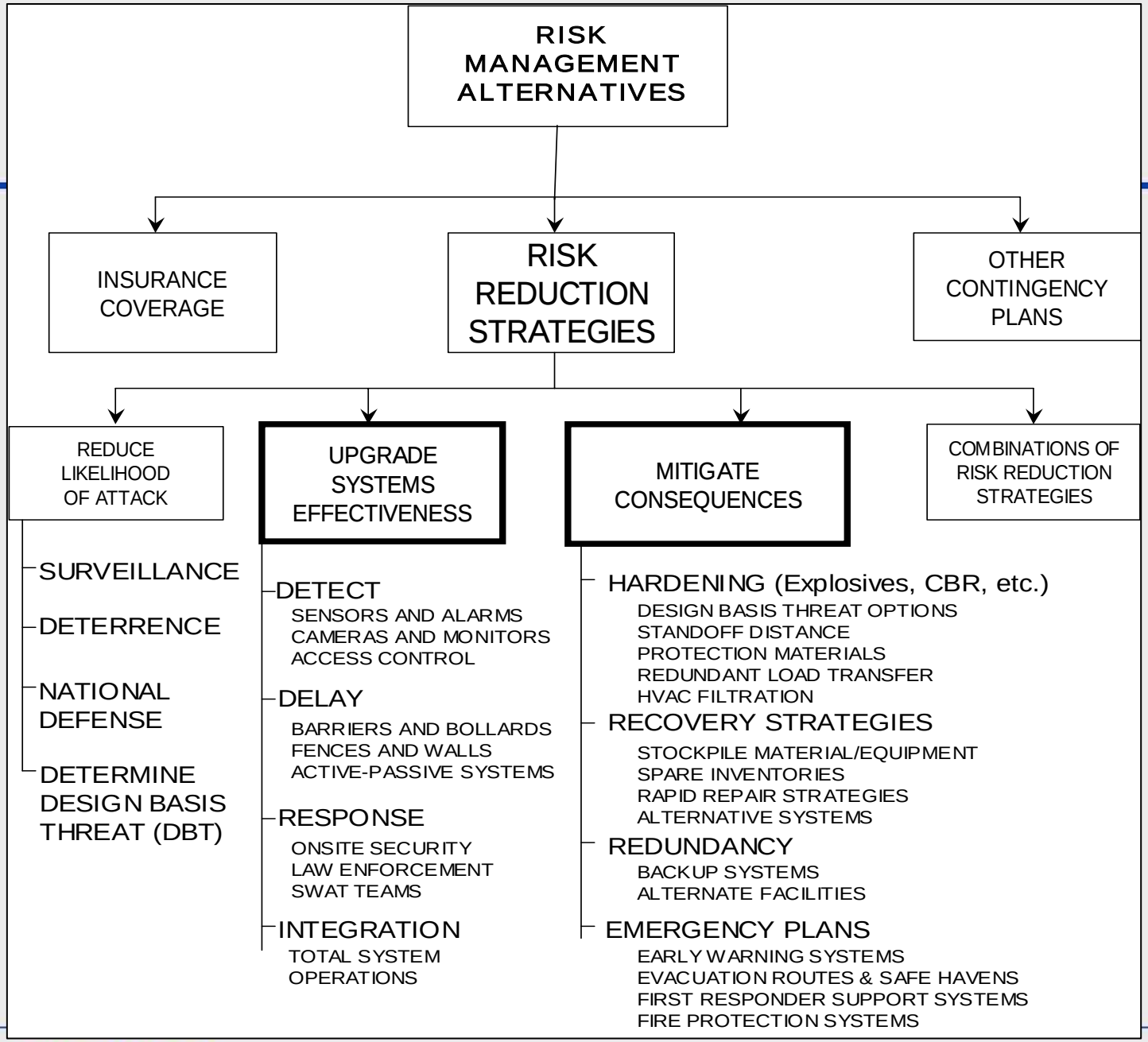
estimation for the likelihood of attack

estimation of terrorist success

estimation of the consequences of a successful terrorist attack

Proposed Security Methodology




RISK MANAGEMENT ALTERNATIVES
INSURANCE COVERAGE
RISK REDUCTION STRATEGIES
OTHER CONTINGENCY PLANS
REDUCE LIKELIHOOD OF ATTACK
UPGRADE SYSTEMS EFFECTIVENESS
MITIGATE CONSEQUENCES
COMBINATIONS OF RISK REDUCTION STRATEGIES
SURVEILLANCE
DETERRENCE
NATIONAL DEFENSE
DETERMINE DESIGN BASIS THREAT (DBT)
DETECT
SENSORS AND ALARMS
CAMERAS AND MONITORS
ACCESS CONTROL
DELAY
BARRIERS AND BOLLARDS
FENCES AND WALLS
ACTIVE-PASSIVE SYSTEMS
RESPONSE
ONSITE SECURITY
LAW ENFORCEMENT
SWAT TEAMS
INTEGRATION
TOTAL SYSTEM OPERATIONS
HARDENING (Explosives, CBR, etc.)
DESIGN BASIS THREAT OPTIONS
STANDOFF DISTANCE
PROTECTION MATERIALS
REDUNDANT LOAD TRANSFER
HVAC FILTRATION
RECOVERY STRATEGIES
STOCKPILE MATERIAL/EQUIPMENT
SPARE INVENTORIES
RAPID REPAIR STRATEGIES
ALTERNATIVE SYSTEMS
REDUNDANCY
BACKUP SYSTEMS
ALTERNATE FACILITIES
EMERGENCY PLANS
EARLY WARNING SYSTEMS
EVACUATION ROUTES & SAFE HAVENS
FIRST RESPONDER SUPPORT SYSTEMS
FIRE PROTECTION SYSTEMS

Proposed Security Methodology

End of presentation

Thank you