COMMISSION INTERNATIONALE
DES GRANDS BARRAGES

VINGT TROISIÈME CONGRÈS
DES GRANDS BARRAGES
Brasilia, Mai 2009

DAMSE: AN EUROPEAN METHODOLOGY FOR RISK BASED SECURITY ASSESSMENT OF DAMS [*]

Ignacio ESCUDER
Civil Engineer, PhD., Universidad Politecnica De Valencia

Manuel G. de MEMBRILLERA
Civil Engineer, PhD., Universidad Politecnica De Valencia

Massimo MEGHELLA
Civil Engineer, CESI Ricerca SPA, Milan, Italy

Armando SERRANO
Civil Engineer, Universidad Politecnica De Valencia

SPAIN

1. INTRODUCTION

Dams are a vital and critical part of Europe's infrastructure, providing extraordinary benefits to society, such as renewable hydroelectric power, flood protection, drinking water, irrigation and recreation. Although, they also represent a public safety issue, for dam failures can result in severe loss of life, economic disaster and extensive environmental damage. Since the events of September 11, 2001, there has been growing awareness of security threats to critical infrastructures and that has resulted in changes to security processes within many industries and regions.

[*] *Damse : une méthodologie européenne pour une évaluation de la sécurité des barrages basée sur les risques*

The DAMSE project has been therefore aimed at developing and verifying a risk-based methodology for the security assessment and management of European dams against threats such as terrorist attacks, sabotage and malevolent intrusions.

2. DAMSE PROJECT PARTERNS AND RESULT DISSEMINATION

Table 1
DAMSE Organizations, role and personnel
Les organisations de DAMSE : rôle et personnel

CESI RICERCA SpA (COORDINATOR-DEVELOPER) http://www.cesiricerca.it Via Rubattino 54, I-20134 Milano-ITALY	Massimo Meghella (project co-ordinator)
UNIVERSIDAD POLITECNICA DE VALENCIA (DEVELOPER) http://www.ipresas.upv.es Camino de Vera s/n, 46022 Valencia-SPAIN	Dr. Ignacio Escuder Bueno (scientific leader) Dr. Manuel G. de Membrillera Ortuño Armando Serrano Lombillo
VERBUND AHP (END USER) http://www.verbund.co.at Am Hof 6a, 1010 Wien AUSTRIA	Dipl.-Ing. Dr. Herbert Schröfelbauer Gerd Schauer Dr. Gerald Zenz Dipl.-Ing. Simone Ortner *Institute of Hydraulic Engineering and Water Resources Management – TU Graz*
CONFEDERACION HIDROGRAFICA DEL JUCAR (END USER) http://www.chj.es Av. Blasco Ibañez 48, 46010 Valencia-SPAIN	Dr. Joaquín Andreu Juan Fullana José Luis Utrillas
C.V.A. – Compagnie Valdôtaine des Eaux SpA (END USER) http://www.cva-ao.it Via Stazione 31, I-11024 Chatillon (AO)-ITALY	Sergio Ballatore Morena Colli
INTERNATIONAL EXPERT PANEL	Dr. Rudolph V. Matalucci *Consultants* Dr. David S. Bowles *Utah State University; RAC Engineerl* Dr. Robin Charlwood *Consultant* Dr. Enrique Matheu *U.S. Department of Homeland Security*

The project entitled DAMSE (A European Methodology for the Security Assessment of Dams) was the object of the Grant Agreement No. JLS/2006/EPCIP/001 of the EPCIP (European Program for Critical Infrastructure Protection). It has lasted from December 2006 to February 2007.

Three important European countries, Austria, Italy and Spain, with more than 30% of all EU large dams, were represented in the DAMSE project, giving it a trans-national nature. Table 1 above shows the main organizations involved, their role, and the personnel that leaded the work.

After 14 months of work, an international workshop was held in the city of Valencia on February 25-26th 2008. The methodology, study cases and reviewers (Expert Panel) point of view were exposed as well as the insights provided by qualified dam stakeholders from 19 countries, and the president of the International Commission on Large Dams (ICOLD). A suitable confidential policy has been adopted to prevent intentional and malevolent access and disclosure of sensitive data and safety related information.

3. REVIEW OF THE STATE OF THE ART

Currently available methodologies on dam security risk management are to be found in the United States. They include the following tools, which provided a robust background to DAMSE project:

a) RAM-D^{SM} and RAM-T^{SM} methodologies developed by Sandia National Laboratories for dams and transmission systems (Ref. [1])
b) DAMSVR developed for FERC by William Foos & Associates for dams
c) MATRIX Security Risk Analysis Program developed by USBR for dams
d) CARVER, a check list approach
e) RAMCAP, Risk Analysis and Management for Critical Asset Protection (Ref.[2])

4. DAMSE METHODOLOGY

4.1. OBJECTIVES

The specific goals of the DAMSE project have been the following:

a) To set forth a procedure for completing a threat assessment that determines the likelihood that an adversary will attack a critical asset to achieve a particular consequence
b) To provide a procedure for completing a consequence assessment should an adversary be successful in disrupting, disabling, or destroying the missions of the entire dam project complex
c) To provide a systematic procedure for determining the vulnerability, that is, the ineffectiveness of the security protection system to prevent a successful attack against an operational component of the dam project
d) To provide the procedure for completing a risk assessment that allows the manager to evaluate the level of risk associated with the threat, consequences, and protective system ineffectiveness and determine the needs for directing an implementation of security upgrades or consequence mitigation for risk reduction, as appropriate for the configuration of the subject dam
e) To verify and demonstrate these procedures on a set of dams, identified following a preliminary screening among the dam portfolio provided by partners

4.2. RISK BASED APPROACH

In addition, it is imperative to bear in mind that risk is a function of several factors, the likelihood of attack, the system ineffectiveness, expressed as the complementary of system effectiveness, and the consequences. Accordingly, the methodology addresses these factors:

$$R = R[P_A, (1 - P_E), C]$$

where:

P_A = Likelihood of adversary attack
C = Consequences of adversary attack
$(1–P_E)$ = Vulnerability or likelihood that adversary attack is successful (its converse, P_E , represents the security system effectiveness in preventing the undesired event)
R = Risk associated with adversary attack

Regarding these risk factors, it is also worthwhile considering the key participants in security risk management, and their roles, as illustrated in Figure 1. Dam owners and stakeholders are legally responsible for dam security and have to decide what actions, if any, should arise from the risk assessment. They are obviously responsible for the actual vulnerability of the dam system. Intelligence communities, that is, law enforcement organizations such as the military and police alike, are the only ones with access to sensitive and precise information on potential threats. Finally, civil protection or emergency agencies are responsible for setting in action government-approved systems and resources whose task is to protect the civilian population in the event of natural, technological or security disasters.

It is clear the connection between Intelligence Communities and the threat component of risk, Dam Owners/Stakeholders and the vulnerability, and Emergency Agencies with the consequences. In any case, the need for collaboration among these key participants must be strongly stressed.

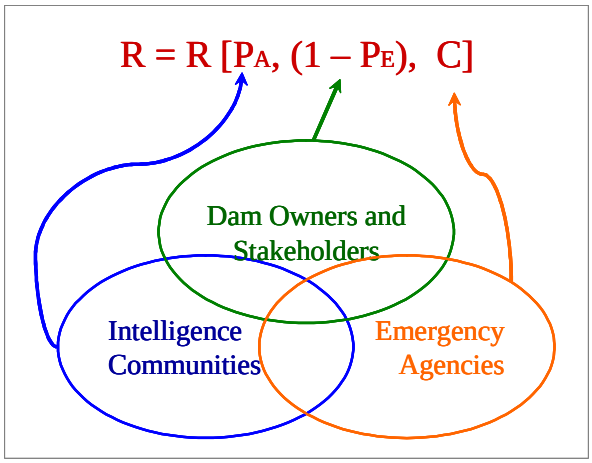

Fig. 1

Collaboration among involved actors and main relationships with risk factors.

Collaboration entre les acteurs impliqués et relations principales avec les facteurs de risque.

The DAMSE security risk assessment and management methodology supports the process shown in the flow chart of Figure 2.

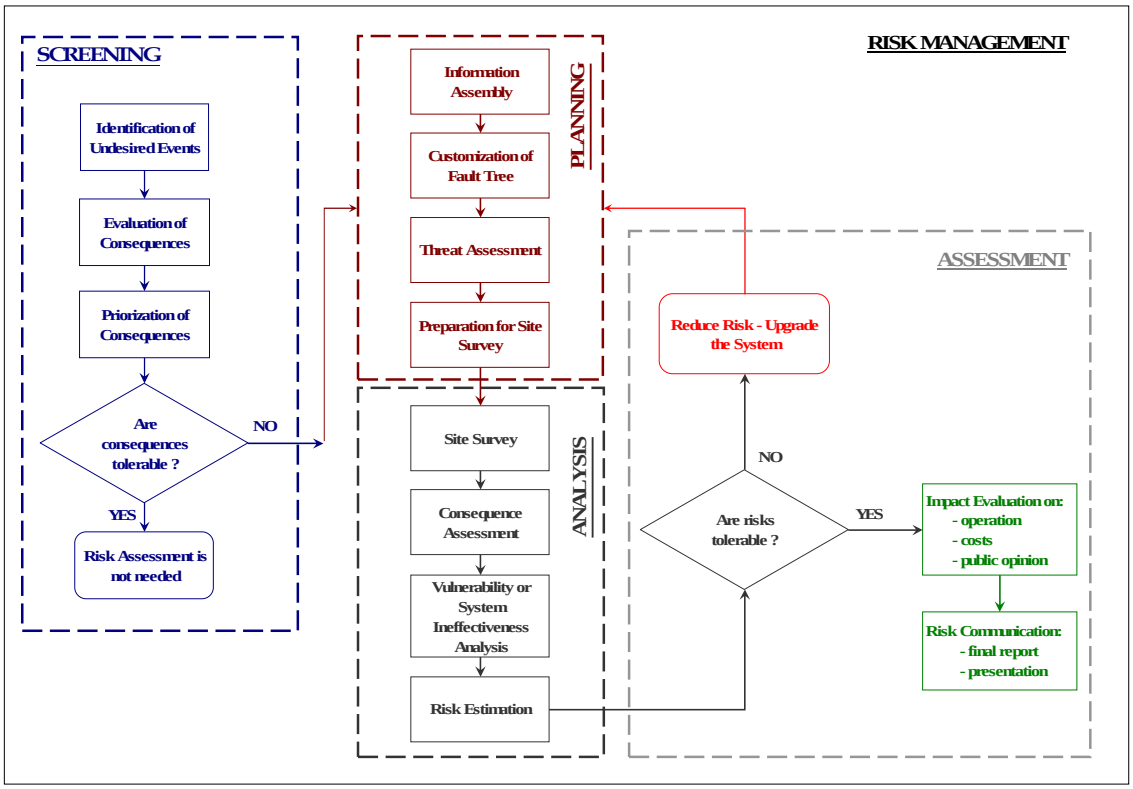

Fig. 2
DAMSE Risk Assessment and Management framework.
Cadre d'évaluation et de gestion du risque de DAMSE.

4.3. STEPS IN THE METHODOLOGY

The process begins with an optional screening profile, based on a simplified consequence assessment, that allows identification of the most critical assets to be subsequently subjected to the full risk assessment.

The initial step of the full risk assessment is to gather and organize all available information on the dam system, including a complete physical description of the facility and a statement of the protection objectives. The next task is to determine what specific assets must be protected to prevent the undesired events from occurring, and these are labeled as critical assets. In complex systems, such as dams, identification of the critical assets is not obvious, and a logic diagram is used to pinpoint all of the ways that undesired events can occur. This diagram is the customized fault tree.

Another step is to analyze the malevolent threats and estimate the threat potential for attack at the dam system, evaluating the event consequences as well. Indications for preparing a site survey are given, and the latter is carried out to collect information from direct observation and interviews with personnel.

Procedures are also included to analyze the effectiveness of the security system against the adversary attack. Finally, a qualitative relative risk is estimated taking into account all risk components at the same time.

In the event that risk is deemed to be above a predetermined threshold, the methodology puts forth a process for identifying risk reduction measures, followed by re-evaluating consequences and protection vulnerability to measure relative risk reductions.

Once the system upgrade has been determined, the impacts of the risk reduction on the mission of the dam and the cost are estimated, looking for trade-offs between risk and total cost whenever it is necessary. The last step in the risk assessment process is to set up a presentation for the risk managers and stakeholders, including all relevant information from preceding steps.

Finally, dam owners/stakeholders must take risk management decisions; in particular, setting the level of threat for which the security system upgrade will be designed, the so-called design basis threat.

4.4. MAIN TOOLS DEVELOPED: SITE SURVEY PROCEDURES AND SYSTEM EFFECTIVENESS ASSESSMENT

The site survey has proven to be one of the most important steps in the methodology and it always gives out important information and useful ideas for later use. Not only external advisors but also site employees take great advantage of the field inspection when it is correctly planned and prepared. All information to be collected has been organized in 8 different worksheets:

- Worksheet 1. Dam data: name, location, type, date of construction, purpose, height, crest length, storage, spillway capacity, freeboard, and a sketch of the dam including all relevant territory and infrastructure upstream and downstream
- Worksheet 2. Dam system layout, including all relevant territory and infrastructure upstream or downstream
- Worksheet 3. List of dam mission and related critical assets
- Worksheet 4. Detailed description of critical assets, including relevant information
- Worksheet 5. Location and description of all physical barriers in the dam system
- Worksheet 6. Location and description of all security systems
- Worksheet 7. Additional miscellaneous information, including emergency planning and procedures, response force available, past security events, etc.
- Worksheet 8. Development of most vulnerable paths to critical assets

The assessment of a system ineffectiveness against and attack should alert the analysis team that the high consequences from that attack might justify some risk reduction attention by the decision makers. It is therefore important that system effectiveness formats be prepared that allow identification of the weaknesses regarding the following elements:

- Detection, which is the sensing, reporting, and assessment of an adversary action
- Delay, as a feature that impedes the adversary to progress in a particular step of its action
- Response, which is the interruption and neutralization of the adversary action by means of physical security and cyber-security measures
- Integration of the preceding factors

It is finally necessary to recall the critical importance of the system fault-tree in the context of security risk assessment, for it embodies all the logic of the problem and outlines the *adversary strategies* to accomplish undesired events. Fault trees help in determining the paths, that is, routes taken by an adversary from off-site through areas and path elements to reach the target and, optionally, to return off-site. Paths are also part of a scenario, which is the outline of events along a specific path by which the adversary plans to achieve his objective.

5. EXAMPLE OF APPLICATION

Evidences of the suitability and utility of the site survey sheets and inspections were provided by demonstrating how fault trees and system effectiveness analysis could be performed from such data by applying the methodology developed.

Tables 1, 2 and 3 show how, for a particular Dam, a specific attack and a critical asset (gated spillway) linked to a particular mission loss (flood control), three different scenarios were assessed:

a) Current (no traffic allowed on the crest)
b) Opening the crest to the traffic
c) Opening the crest to the traffic and security improvement.

In the provided tables, information was gathered from the different worksheets (WS): *Detection Effectiveness* was assessed from data in WS#6 and WS#4, *Communication Reliability* was assessed from data in WS#7, *Delay Time* was assessed from data in WS#5 and WS#8 and *Response Time* was assessed from data in WS#7. Each assessment qualification is done in terms of VH (Very High), H (High), M (Medium), L (Low) and VL (VL). Finally, “Delay” time is not the sum of all partial times and an algorithm accounts the likelihood of “detecting” the

attack in different moments. Figure 3 shows the upper portion of the fault tree developed for the above dam mission loss (flood control)

Table 1

System effectiveness analysis for situation 1 (current): no vehicular or pedestrian transit allowed on crest

Analyse d'efficacité du système pour la situation 1 (actuelle) : crête interdite aux véhicules et aux piétons

Gated Intermediate Spillway

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into restricted area through gate D2	VH		60 s			
Get to door D7 through the crest by car = 500m	M		30 s			
Break into door D7	L		90 s			
Get to valve chamber on elevator	NA		180 s			
Task	L		720 s			
Total	**M**	**H**	**1047 s**	**1500 s**	**M**	**M**

Table 2

System effectiveness analysis for situation 2: transit allowed on crest.

Analyse d'efficacité du système pour la situation 2 : trafic autorisé sur la crête.

Gated Intermediate Spillway

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into restricted area through gate D2	NA		0 s			
Get to door D7 through the crest by car = 500m	NA		0 s			
Break into door D7	L		90 s			
Get to valve chamber on elevator	NA		180 s			
Task	L		720 s			
Total	**L**	**H**	**855 s**	**1500 s**	**L**	**L**

Table 3

System effectiveness analysis for situation 3: transit allowed on crest plus implementation of door sensors and emergency protocols

Analyse d'efficacité du système pour la situation 3 : trafic autorisé sur la crête avec mise en place de capteurs et de protocoles d'urgence.

Gated Intermediate Spillway

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into restricted area through gate D2	NA		0 s			
Get to door D7 through the crest by car = 500m	NA		0 s			
Break into door D7	VH		90 s			
Get to valve chamber on elevator	NA		180 s			
Task	L		720 s			
Total	**M**	**VH**	**977 s**	**900 s**	**M**	**M**

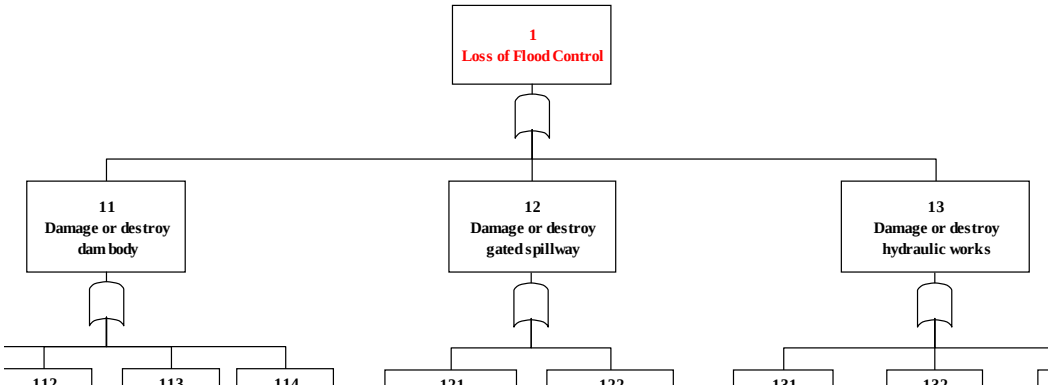

Fig. 3
Upper portion of the flood control loss fault tree
Partie supérieure de l'arbre de défaillances concernant la maîtrise des crues.

CONCLUSSIONS

The key findings, conclusions, and recommendations that stem from the DAMSE project are the following:

a) The verification of the methodology through its application on nine large dams, dealing with different organizations and conditions, has proven to be a major contribution of the project. This has also provided the methodology with the sufficient flexibility to adapt to a wide variety of circumstances, making it applicable to any dam.

b) The current security measures seem not fully justified and/or not based on rationale and comprehensive assessment. The methodology systematically pinpoints the issues that need priority attention and identifies critical assets within a dam system. Moreover it generates structured documentation that leads to repeatable results and provides defendable records in case of liabilities after an attack.

c) Significant improvement in security levels can be achieved at a considerably lower cost than for upgrading safety.

d) Security risk is difficult to quantify, especially because predicting human behavior may never be a random event in the mathematical sense. Computational modeling of threats aimed at providing a numerical estimate of threat probability, is still not fully reliable and not directly applicable, due to inherent high level of uncertainty and limitations.

e) Redundancy is a key concept to effectively improve both security and safety, even if it is difficult to afford and manage security and safety in a common framework, which, anyway, should be definitely pursued.

f) The security risk value obtained with the DAMSE methodology is a qualitative estimate that must be checked considering all three risk components: threat, vulnerability and consequences.
g) Numerical modeling can effectively support vulnerability analysis, but more research efforts are needed, e.g. to evaluate explosives effects.
h) More effective and cheaper protection against terrorist attacks can be achieved if security issues are properly addressed at the design stage.
i) The methodology has practical implications, for it gives a systematic basis for security management decision making. Dam security should be addressed on a regular basis, in a similar way as dam safety.
j) Integration and coordination between facilities owners, security experts, social scientist, police, intelligence and authority is of paramount importance.
k) The methodology provides with a standardized baseline and a common risk terminology that could be adopted by all stakeholders and become the first step of a common framework for the effective protection of dams at EU level.

ACKNOWLEDGEMENTS

Special mention is due to the European Commission for the received support and all other partners in the project, namely the End Users and Panel Review Members, for their invaluable contribution and effort.

REFERENCES

[1] MATALUCCI, R.V. *"Risk Assessment Methodology for Dams"*, In Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management (PSAM6), Vol. I, pp.169-176; USA 2002.
[2] ASME Innovative Technologies Institute, LLC. *"RAMCAP: Risk Analysis and Management for Critical Asset Protection – The Framework"* Version 2.0; Washington DC, 2006.

SUMMARY

Dams are a vital and critical part of Europe's infrastructure, providing extraordinary benefits to society. They also represent a public safety issue, for

dam failures can result in severe loss of life, economic disaster and extensive environmental damage. The DAMSE project has been therefore aimed at developing and validating a risk-based methodology for the security assessment and management of European dams against threats such as terrorist attacks, sabotage and malevolent intrusions. The objective has been pursued through the beneficial cross-interactions among qualified end-users (dam owners/authorities) and developers (dam engineering specialists), joined in a trans-national team from Italy, Spain and Austria.

RÉSUMÉ

Les barrages jouent un rôle vital au cœur de l'infrastructure de l'Europe et offrent à la société des avantages incroyables. Ils représentent toutefois un problème de sûreté publique en cas de rupture, entraînant ainsi d'importantes pertes humaines, économiques et écologiques. Le projet DAMSE a donc pour but le développement et la formalisation d'une méthodologie basée sur les risques pour l'évaluation de la sécurité des barrages face aux attaques terroristes, au sabotage ou aux intrusions malveillantes. Pour atteindre cet objectif, des interactions croisées pertinentes entre les utilisateurs finaux compétents (propriétaires de barrage/autorités) et les responsables du développement (spécialistes d'ingénierie de barrage), réunis au sein d'une équipe transnationale regroupant l'Italie, l'Espagne et l'Autriche.