DAMSE Expert Panel Review Comments

David Bowles, Robin Charlwood, Enrique Matheu, Rudy Matalucci

at the

Universidad Politecnica de Valencia

Tuesday, February 26, 2008

Outline of Review

- **Introduction**
- **Part I – Compliance of Achieved vs Expected Results**
  - **Relative to Technical Annex - Grant Application**
  - **Relative to CESI-RICERCA Report Section 4 – Design Basis**
- **Part II – Quality and Innovation Level of Results**
  - **Deliverable 1 – Preliminary Screening Procedure (Report)**
  - **Field Manuals for Site Surveys – (3 Reports)**
  - **Deliverable 3 – Methodology (PPT and TOC)**
  - **Deliverable 4 – Verification (TOC)**
- **Part III – Limitations, Defaults & Improvement Needs**

INTRODUCTION

Documents Reviewed:

- Terms of reference of DAMSE project
- Terms of reference of Expert Panel Review
- CESI-RICERCA Report Feb 2007
- Documentation Provided Aug 2007:
  - Screening Procedure,
  - Field Manual
  - Fault Trees
- Feb 25th 2008 Workshop Presentations and Lessons Learned

Part I – Compliance of Achieved vs Expected Results

Relative to Technical Annex - Grant Application

- Section 2.2 - Content

– Security is a hot critical issue/lack of systematic approach/risk methodologies/need to technical and decision tools

– Develop threat +consequences+ system effectiveness+ risk assessment procedures and validate on a set of dams

– Innovative risk based approach required to achieve wide acceptance

– Added value at EU level as a model of “best practices” being widely applicable

– Procedure will address: **Preliminary Screening + Risk Assessment**

– Procedure will not address: Risk Management + Emergency Management

- Section 2.3 – Results, Evaluation & Dissemination

– European Security Assessment Methodology including
  - Simplified procedure fro preliminary screening
  - Full security risk assessment procedure
  - Confidential Report

– End-Users get a partial security assessment of their dams portfolio

– European dam operators, authorities and engineers will have a framework

– All project results will be disseminated via workshop, NW-IALAD, ICOLD etc

Part I – Compliance of Achieved vs Expected Results

Relative to CESI-RICERCA Report Section 4 – Design Basis

1. The risk assessment methodology and security risk management system design will use the well known safety and security principles of fault tree and event tree analysis, risk analysis procedures and processes applied to dams and power grids
   - **It does all these**
2. Rigorous risk-based security assessment methodology
   - **The logic is based on risk concepts – current analysis is qualitative not quantitative**
3. Consistent basis for accepting theoretical and empirical system performance data from multiple sources
   - **Can incorporate tecniques from safety assessments etc**
4. Systematically derived risk levels for decision making
   - **Structured system for estimating risk levels**
5. Standardized baseline and common risk terminology with all stakeholders
   - **Uses existing risk factors and includes comprehensive list of definitions**
6. Repeatability of results where same input data is applied
   - **To be evaluated**

Part I – Compliance of Achieved vs Expected Results

Relative to CESI-RICERCA Report Section 4 – Design Basis

7. Can be customized to meet the appropriate scope and level of effort for the project through a screening and subsequent selection of required level of more detailed analysis
   - **Includes a Screening Procedure based on consequences**
   - **Methodology to select various levels of full risk analysis to follow**
8. Provides records for accountability by the decision-makers of:
   - Assumptions/Decisions/Acceptable risk levels determined by owners/stakeholders
   - **Documents, tabulations, FTs etc will define basis. Acceptability to be decided**
   - Implementation of any required security enhancements
   - **Shows benefits to system effectiveness and qualitative risk from upgrades**
9. Includes Guidelines for management of confidential information by the various stakeholders **– To come**
10. Traceable path of assessment data and risks considered
    - **Project data and analyses are all recorded and transparent**
11. Defendable record in event of liabilities after an attack
    - **Data and analyses will be recorded and transparent in full assessments**

Part I – Compliance of Achieved vs Expected Results

Relative to CESI-RICERCA Report Section 4 – Design Basis (cont)

12. Internal verification and external validation that the methodology meets the above requirements via test applications at relevant project sites
    - **"Verification projects" address this conceptually**
13. Includes Quality Assurance/Quality Control recommendations for applications
    - **Not yet?**
14. Designed to facilitate automation
    - **To be discussed. Would greatly assist upgrade design optimization**
15. Designed to facilitate periodic security assessment updates at projects
    - **Documentation provides a basis for this. Automation would assist**
16. Designed to facilitate future integration with safety and reliability analyses
    - **Use of risk logic allows this but need to decide if prudent to combine information**
    - **Safety analysis uses natural hazards information**
    - **Security analysis uses human threat information which can be used adversely**
    - **Consider establishing a Security Protocol/Licensing Control for DAMSE**

Part II: Quality and Innovation Level of Results

Overall Methodology

- **Preliminary Screening – Deliverable 1 (Report +PPT)**
- **Risk Assessment – Deliverable 3 (based on PPT)**
- **Field Manuals for data collection (examples)**
- **Risk Management – not in scope**
- **Emergency Management – not in scope**

Part II: Quality and Innovation Level of Results

Deliverable 1 – DAMSE Preliminary Screening Procedure

- **Screening approach used to identify "most critical" facilities within a given portfolio.**
- **Consequence-based approach using ordinal descriptors obtained based on ranges of relevant parameters or qualitative descriptions.**
- **Follow-on security risk assessment recommended if screening renders "MEDIUM" or "HIGH" results.**
- **Final portfolio ranking essentially driven by total numerical scores: consequence scores are added**
- **Glossary definition as initial step in the development of the methodology:**
  - **Mission Objective = Project purpose (Flood Control ≠ Reservoir Retention)**
  - **Dam-Break Affected Zone = Flood Inundation Zone? (not necessarily identical)**
- **Screening based on available information (Dam Safety sources).**

Part II: Quality and Innovation Level of Results

Deliverable 1 – DAMSE Preliminary Screening Procedure

- **Consequences:**
  - **Public Safety Consequences (Population at Risk)**
  - **Economic Consequences (Definition?)**
    - **Direct losses (residential, commercial, & industrial property, other infrastructure)**
    - **Repair/Replacement**
    - **Emergency Response & Recovery**
    - **Clean-up cost (not environmental restoration)**
  - **Environmental Consequences**
- **Consequences defined according to ordinal descriptors (VL, L, M, H, VH) associated to parameter ranges.**
  - **Ad-hoc upper limits (No constant ratios)**
- **Relation between ranges for PAR and residential (property damage):**
  - **HIGH PAR = 1,000~5,000 people / HIGH RESIDENTIAL = 10~50 houses destroyed**

Part II: Quality and Innovation Level of Results

Deliverable 1 – DAMSE Preliminary Screening Procedure

- **5 failure scenarios (total failure + facility disruption):**
  - **Loss of Flood Control or Retaining Capacity**
  - **Loss of Hydroelectric Generation**
  - **Loss of Water Supply & Irrigation**
  - **Loss of Recreation/Tourism**
  - **Loss of (Commercial) Navigation**
- **In general**
  - **Loss of Flood Control ≠ Loss of Retaining Capacity ("Uncontrolled" Release).**
  - **Flood control is related to a benefit provided by the project and it is quantified by the mitigation of flood-related damages.**
  - **Loss of Hydroelectric Generation → It may also result from Loss of Retaining Capacity (in case of failure and loss of reservoir).**
- **Mission criticality not considered explicitly since all estimates for mission specific scenarios are evaluated in terms of economic indicators.**

Part II: Quality and Innovation Level of Results

Deliverable 1 – DAMSE Preliminary Screening Procedure

- **Scope Evaluation and Approvals by Management**
  - **How much Data is Necessary for Screening?**
  - **Consider long term data management**

Part II: Quality and Innovation Level of Results

Field Manuals for Site Surveys

DAM AND HYDROPOWER PLANT SYSTEMS LAYOUT

- **Identification of primary and secondary missions (purposes) and supporting functions:**
  - **Hydropower generation (links to transmission systems)**
  - **Potable water supply (links to aqueducts, canals, pumping stations, water treatment systems)**
  - **Agricultural and industrial water supply (links to aqueducts, canals, pumping stations)**
  - **Flood damage reduction (typically part of a larger system)**
  - **Recreation**
  - **Navigation**
  - **Wildlife & fish**
  - **Retention of hazardous materials**
- **Determination of facility layout must incorporate local and regional setting information, including identification of potential off-site response/prevention forces.**

Part II: Quality and Innovation Level of Results

Field Manuals for Site Surveys

DAM AND HYDROPOWER PLANT SYSTEMS LAYOUT

- **Identification of critical infrastructure that provides direct support to the facility or that could be potentially affected by its failure or disruption:**
  - **Downstream Dams**
  - **Power Generation Facilities**
  - **Oil/Gas Processing, Storage, and Transport Facilities**
  - **Electricity Transmission and Distribution Facilities**
  - **Major Highways, Bridges, Tunnels, and Airports**
  - **Ports and Inland Waterways**
  - **Telecommunication Facilities**
  - **Chemical Plants**
  - **Waste Water Facilities**
- **Data collection process must consider the corresponding information protection issues (distribution and storage of sensitive information).**

Part II: Quality and Innovation Level of Results

Deliverable 3 – Methodology (Risk Assessment)

SECURITY RISK ASSESSMENT PROJECT PREPARATION

- **Scope Evaluation and Approvals by Management**
  - **Where to Place the Emphasis**
- **Budget Arrangements and Schedules**
- **Site Survey Procedures (Drawings, Data Acquisition, Documentation, etc.)**
- **Selection and Commissioning of Risk Assessment Team**
  - **Disciplines and Numbers Required**
  - **Size of Project and Time Constraints**
  - **Training must be Included**

Part II: Quality and Innovation Level of Results
Deliverable 3 – Methodology

SECURITY RISK ASSESSMENT PROJECT PREPARATION (cont)

- **Critical asset characterization should be based on evaluation of technical details and operational processes that identify critical elements supporting a passive or active function for the facility.**
- **Critical assets may include not only those on the facility but also may consider surrounding and supporting infrastructure.**
- **Analysis will require identification of existing layers of protection**
- **Analysis may include identification of replacement and quick repair strategies.**
- **Significant relevant information may be available from previous dam safety assessments.**

Part II: Quality and Innovation Level of Results

Deliverable 3 – Methodology

SITE SPECIFIC DATA PRESENTATION*

- **Generic Fault Trees and Customizing Procedures**
- **Identification of Critical Assets and Consensus**
  - **Show on Fault Tree**
- **Identification of Potential Adversarial Attack Scenarios (Paths)**
  - **Document also on Fault Tree where possible**
- **Discovery of Obvious System Weaknesses and Concerns**
  - **More Objective with Analysis Procedures**
- **Identification of Dam/Plant Redundancy Systems**
  - **Show as AND Gates**

* Also Covered Previously under Field Manuals

Part II: Quality and Innovation Level of Results
Deliverable 3 – Methodology

THREAT ASSESSMENT

- **Threat Spectrum Procedures**
  - **Provide/Apply Broad Threat Reference Table**
- **Methodology for Reaching Consensus on Potential Site Specific Threat (s)**
  - **Consider "what-if" scenarios**
- **Likelihood of Attack and Rating Procedures**
  - **Attractiveness, Ease of Attack, Largest Impact, Motivation, Local Intelligence**
  - **Check CARVER Approach for "some" Additional Parameters**
- **Inputs & Confirmation from Intelligence Community**
  - **Law Enforcement**
  - **Government Agencies, Local Authorities**
  - **Jurisdictional Extent**
- **Selection and Approval of Most Reasonable Design Basis Threat**
  - **With Decision-Maker using Technical Evaluations**
  - **Analyses of Damage and Consequences (Manageability)**

Part II: Quality and Innovation Level of Results
Deliverable 3 – Methodology

SYSTEM EFFECTIVENESS ANALYSIS

- **Existing Physical Protection System Description (OK)**
- **Site Specific Detection, Delay, Response (and Neutralization Effectiveness), Systems Integration**
  - **Personnel, Technology, and Hardware**
  - **Time-Line Analysis Helpful**
- **Access Routes (Water, Land, Air)**
- **Off-Site Surveillance Equipment/Agencies (Documented)**
- **Confirm Developed Evaluation/Rating System (In-Place Application Noted)**
- **Analysis Procedures (Judgment, Consensus, Skills of Analysts)**
- **System Effectiveness Evaluation Results and Consensus Procedures**
  - **High (H), Medium (M), Low (L)**

Part II: Quality and Innovation Level of Results

Deliverable 3 – Methodology

CONSEQUENCE ASSESSMENT

- **Define estimate consequences for the "Worst Reasonable Case"**
- **Recommend keeping natural units for consequences (i.e. € and fatalities) and avoid transforming to scores**
  - **This avoids distorting the significance of consequences**
  - **It facilitates relative cost effectiveness estimation for security upgrades**
- **The significance of third party consequences is a societal matter whereas the dam owner should determine its risk tolerance for financial losses**
- **Consideration of Life Loss instead of PAR would allow:**
  - **Accounting for the effects of differences in warning time for attack modes**
  - **Accounting for the potential benefits from security upgrades that increase warning time**
- **"Loss of Flood Control" currently combines two different types of consequences, which should be separated:**
  - **Loss of Flood Control as a project benefit**
  - **Breach of the dam by a malevolent act**

Part II: Quality and Innovation Level of Results
Deliverable 3 – Methodology

RISK ANALYSIS

- **The "Risk Equation" that multiplies probability and consequences is for calculating an average risk**
- **Recommend separate evaluation of Threats, System Effectiveness and Consequences**
- **Consideration of the cost effectiveness of security upgrades would require estimation of probabilities instead of scores to characterize threat and system effectiveness but the threat probability is not currently amenable to quantification.**
- **Conditional risk estimates for loss of mission can serve a value purpose in identifying opportunities for security upgrades.**

Part II: Quality and Innovation Level of Results
Deliverable 4 – Verification

- Verification of risk assessment methodology on 8 dams initiated and in process
- Procedures demonstrated
- Preliminary results under review
- Accomplishments within the budget are commendable

Part III: Limitations, Defaults and Improvement Needs

- Screening procedures are applicable for identifying highest priority dams
- Full procedure is required for risk assessment and prioritization of security upgrades
- Completion of the risk assessment verification phase will provide useful insights
- Project will benefit from inclusion of the
  - Emergency response organizations for the public safety consequences assessment factor
  - Intelligence community, particularly for the threat assessment factor

Acknowledgements

The Panel thanks the Project Team for providing us the opportunity to offer review comments on this important project.

The team is complimented on the project documentation and their comprehensive presentations on February 25th, 2008.

We hope that the above comments are of value to the project.