Current US Security Practice for Hydro Facilities

Outline of Presentation

- Responsibilities of FERC and Owners for security of US hydro projects
- FERC's Security Program for Hydro Projects
- Owners Security Assessments and Actions Required by FERC
- Current status of FERC
- Vulnerability Assessment Methodologies - VA Analysis, DAMS-VR, RAM-D, RAM-T
- RAM-D and RAM-T Methodologies
- RAMCAP

Robin Charlwood &
Rudy Matalucci

Responsibilities for Security at US Hydropower Projects

- Federal dams
  - US Bureau of Reclamation (USBR) 471 dams, US Army Corps of Engineers 660 dams, etc.
- Non-federal dams for hydropower
  - Federal Energy Regulatory Commission (FERC) 2500 dams.
- Other dams
  - State Dam Safety Officials .

FERC Security Program for Hydropower Projects

- Program was distributed to licensees/exemptees in June 2002.
- FERC received comments and recommendations from licensees and other agencies.
- FERC Issued Revision in November 2002
- All Licensees responded to FERC by September 30, 2003
- Security measures have been implemented

Owners Security Assessments Actions Required by FERC

Licensees/exemptees will be responsible for:

- Security at their projects, vulnerability and risk assessments of their projects (as appropriate), security upgrades, and communicating with local law enforcement and nearby dam operators.
- Having a single designated contact to receive FERC security alerts.
- Having a designated contact to the FERC for other security related communications.
- Ensuring that the corporate security officer be involved with all security associated activities.
- Making sure that security measures do not conflict with License requirements.
- Integrating the EAP, Security Plan, and Recovery Plan for their projects, if that project has those documents.
- Communicating to the FERC Dam Safety staff and nearby dam operators regarding security breaches or incidents, if not expressly restricted by law enforcement agencies.

Requirements for FERC dams:

Requirement	Group 1	Group 2	Group 3
Security Assessment	Yes (1,4)	Yes (1,4)	No (2)
Vulnerability Assessment	Yes (1,5)	No (2,5)	No (5)
Security Plan	Yes (1)	Yes (1)	No (2)
Integration of Security concerns and EAP procedures	Yes (3)	Yes (3)	No (2)

1 Completed by September 30, 2003.

2 Although not required, this item is strongly encouraged.

3 Integration should begin immediately, and be revised as conditions change and documents are refined or developed.

4 A separate Security Assessment may not be required for a dam if a more detailed Vulnerability Assessment is completed for that facility that addresses the need for security upgrades.

5 A Vulnerability Assessment must be completed prior to the FERC approval of requests for permanent closures of recreational, or other project, facilities.

Documents Required by FERC

Security Assessment - An evaluation of the current state and appropriateness of the onsite security system and what needs to be done at a project or facility to address concerns regarding security, such as installation of fences, gates, cameras, increased guards, etc.

This assessment will identify if any security enhancements are needed, and specifically what those enhancements consist of. The recommendations made from the Security Assessment will lead to improved security measures and should be incorporated into the corporate Security Plan (see definitions, below).

Documents Required by FERC

Vulnerability Assessment (VA) - *addresses the following:*

1) it identifies the "weak points" or vulnerable project features;

2) it assesses the potential threat to a facility as based on organizations or people who may wish to cause harm to the facility, a history of security incidents, and information received from the FBI or other law enforcement agencies specific to your area or facility;

3) it addresses the consequences of such an attack, and;

4) it addresses the effectiveness of the security system to counter such an attack. These factors should be addressed with a fair degree of confidence, with some supportive documentation to substantiate the assumptions.

VAs must be completed for all Security Group 1 Dams, and for any dams where there is a request to close usage (i.e., recreation or roads) of project lands for security reasons.

A Security Assessment may be incorporated within a detailed VA.

Documents Required by FERC

Security Plan - A document that characterizes the response to security concerns at a project or facility.

The Security Plan may include specific features of the project security program, such as fences, surveillance cameras, etc. and company procedures to follow based upon changing threat conditions or situations.

The Security Plan can be very simple or very complex based upon the specifics of the site as well as the assessment of the potential threat to the facility.

Documents Required by FERC

Recovery Plan - A document describing the actions an organization will take to recover from a disaster. The disaster can be natural or caused by criminal activity.

A Recovery Plan in this program generally refers to the pre-planned actions allowing a utility to continue, or quickly restore, generation of power, or otherwise function in its intended purpose.

This document is also known as Utility Recovery Plans, Continuity of Operation Plans, etc. This document can be specific to a hydropower dam or reservoir, and/or part of the entire utility company recovery plan.

Documents Required by FERC

Emergency Action Plan (EAP) - A document describing the actions a dam owner/operator takes if a problem exists at a dam, whether due to natural causes or sabotage.

Actions include identifying and assessing the problem, mitigating the problem if possible, and notifying the emergency management system to protect human life and property.

Inundation studies and notification call charts are included in EAPs.

Documents Required by FERC

Integration of plans - In this program, "integration" of plans is defined as ensuring that there is continuity between the many company documents that may exist, such as Security Plans and Emergency Action Plans (EAPs). Emergency and response actions arising from procedures contained in company documents should be internally consistent, with few if any procedural conflicts. Authors and administrators of documents within a company should ensure that proper coordination has been achieved and, as an example, the security personnel understand the procedures contained in the EAP and vice versa.

"Integration" does not mean that security information should be incorporated into an EAP, which would have a wider distribution than a Security Plan.

RESULTS OF FERC LICENSEE VULNERABILITY/SECURITY ASSESSMENTS

Licensees Completed Vulnerability/Security Assessments on Sept 30, 2003

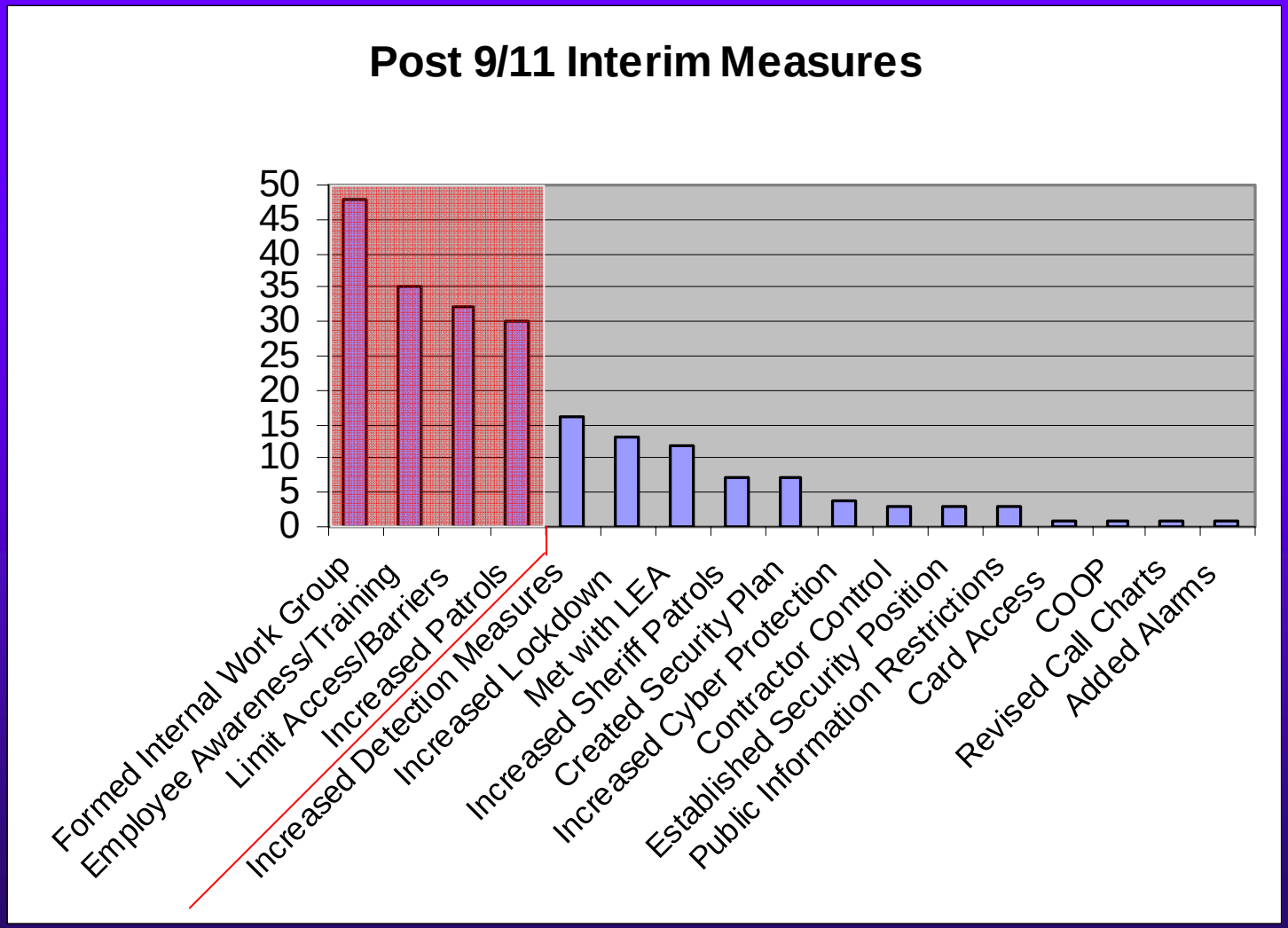
FERC received 273 Summary Reports for the September 30, 2003 Deadline (many reports cover multiple dams).

- **All Security Group 1 and Group 2 Dams (1,050) Completed Studies**
- **Used to Assess and Upgrade Security Where Necessary**
- **Used as Baseline for Future Needs**

The following are cumulative results learned from the submittals:

Robin Charlwood &
Rudy Matalucci

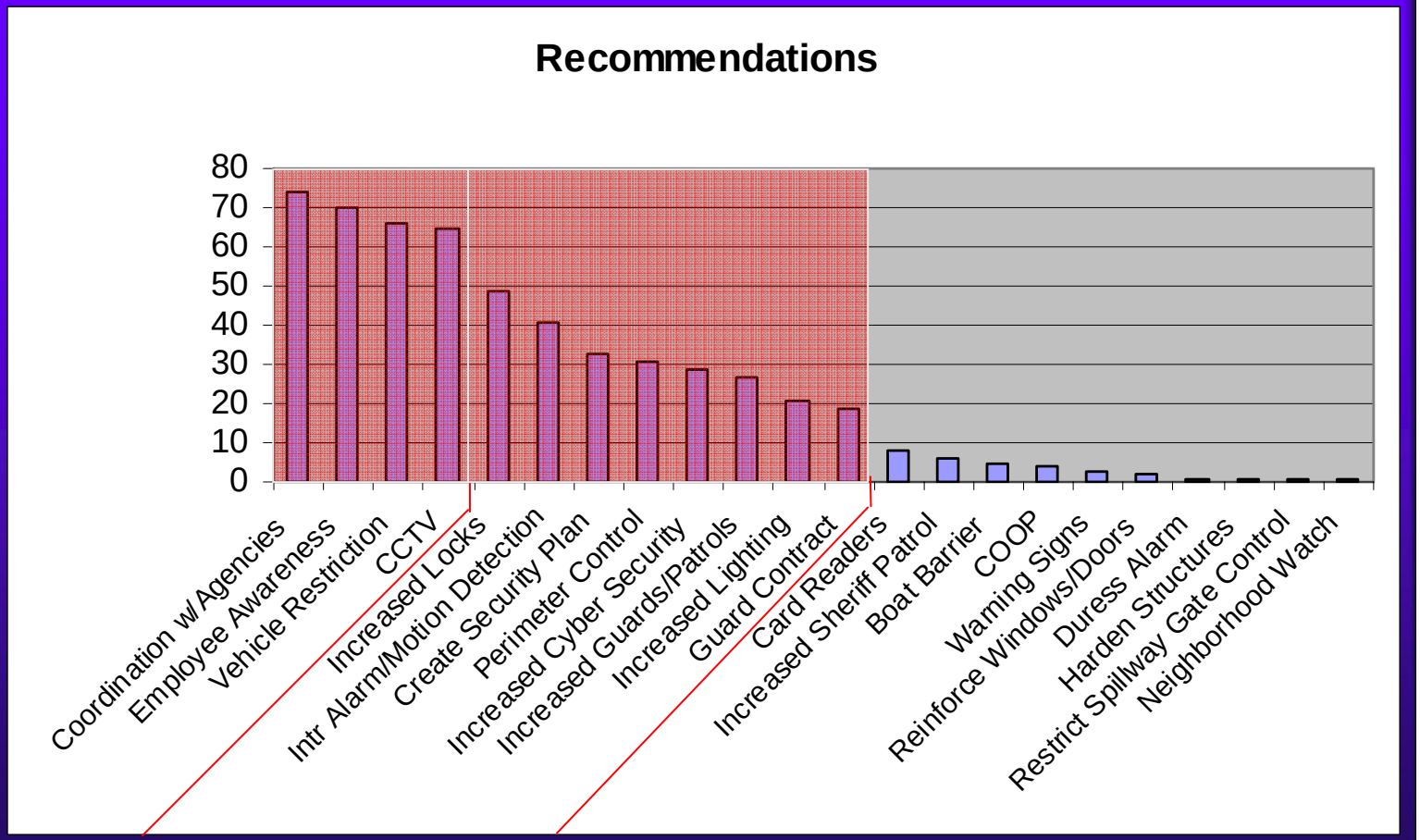
RESULTS OF LICENSEE VULNERABILITY/SECURITY ASSESSMENTS



Robin Charlwood &
Rudy Matalucci

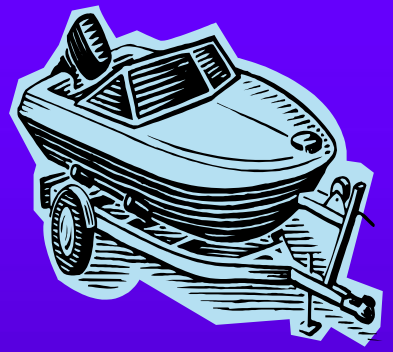
RESULTS OF LICENSEE VULNERABILITY/SECURITY ASSESSMENTS

What Were the Suggested Upgrades Identified by the Assessments?



An Issue - Recreation at Hydropower Projects

What does this mean for licensees and recreational access at FERC Hydropower Projects?



Robin Charlwood &
Rudy Matalucci

RECREATION REQUIREMENTS

In addition to approved recreation plans-

Licensees are required to provide free public access, to a reasonable extent, to project waters and adjacent project lands … for the purpose of full public utilization of such lands and waters for navigation and for outdoor recreation purposes… (L-forms)

Provided, that the licensee may reserve from public access such portions of the project water, adjacent lands, and project facilities as may be necessary for the protection of life, health, and property.

What Can A Dam Owner Do?

- Provide additional security measures including personnel, lights, and cameras
- Work closely with local law enforcement agencies to coordinate security
- Work with local recreation groups

Options to Permanent Closure

Closures based on specific threat

Robin Charlwood &
Rudy Matalucci

Options

- Relocate a facility further from the dam or vulnerable area in order to provide public access

  Example- A licensee relocated its visitor center further from the perceived vulnerable area in order to continue to provide educational programs

- Opening access points during specific times such as peak weekends, special events, and holidays.

Points To Consider

- Stay alert and informed.
- Notify appropriate Regional office and the Washington office of changes at the project.
- Review and revise, where appropriate, the signage at the project to reflect any changes to the public access at the projects.
- Attend local community meetings, meetings with local recreation groups such as anglers or whitewater rafting groups.
- Put notices in the local newspapers in order to inform the public of changes.

Vulnerability & Risk Assessment Methodologies

- VA Analysis – simplified method proposed by FERC in April 2003 – available for use by Owners
- DAMS-VR – method proposed by FERC for staff monitoring of Licensees Security Programs – available from FERC on a controlled basis
- RAM-D, RAM-T & RAM-W – by Sandia Labs
- RAMCAP

VA Analysis (Simplified Ram-D)

I. Threat Analysis (T)

1. Determine the presence and motivation of a Threat
2. Does the above group have personnel/resources sufficient to carry out the failure consequences (specific targets to be identified in Steps 4 and 5)?
3. Estimate number of attackers, equipment, tools, vehicles, weapons, and tactics for each group

VA Analysis (Simplified RAM-D)

II. Consequences (C)

4. Life Loss
   - 4A. Dam Failure
   - 4B*. Vulnerable Feature (i.e., Gate) Failure
5. Dam Mission (Power, Water Supply, Flood Control, Navigation, Environmental)
6. For each group (from Step 2) record both Life Loss Consequences:
7. For each group (from Step 2) record both Dam Mission Consequences
8. Record the highest of above four Consequences for each group identified from Step 2 (Low, Medium or High)

VA Analysis (Simplified Ram-D)

III. Security System Effectiveness (S)

9. Estimate Detection/Assessment Ability (DA):
   Low Medium High
10. Estimate Delay Time (time from first detection to action causing failure) (DT = minutes)
11. Estimate Effective Response Time (time from first detection to deployment of sufficient response force) (RT = minutes)

VA Analysis (Simplified Ram-D)

III. Security System Effectiveness (S) continued

12. Determine Security System Effectiveness (from Steps 9, 10, and 11)

	DA=Low	DA =Medium	DA=High
DT < RT	Low (S)	Low (S)	Medium (S)
DT > RT	Low (S)	Medium (S)	High (S)

VA Analysis (Simplified Ram-D)

III. Security System Effectiveness (S) continued

13. Compare maximum Consequence (C) (Step 8) for each identified group to the Security System Effectiveness (S) (Step 12) to determine the Attack Potential (AP) for that group:

	Low (S)	Medium (S)	High (S)
Low C	AP = 1	AP = 1	AP = 1
Medium C	AP = 2	AP = 1	AP = 1
High C	AP = 3	AP = 2	AP = 1

If the Attack Potential is “1” for all groups, then no further analysis is necessary. If the Attack Potential is “2”, or “3” for any group, then compare it to the Threat Analysis for that group.

VA Analysis ("Simplified Ram-D")

III. Security System Effectiveness (S) continued

14. Compare Attack Potential (AP) (Step 13) to Threat (T) (Step 2) for each identified group:

	Low Threat (T)	Medium Threat (T)	High Threat (T)
AP = 1	**No**	**No**	**No**
AP = 2	**No**	**No**	**Yes**
AP = 3	**No**	**Yes**	**Yes**

If "Yes", security enhancements are strongly suggested; continue with a Security Assessment. If "No", security enhancements may not be needed unless the Threat Level increases for that group. Develop unified security upgrades to address the identified weaknesses and vulnerabilities.

DAMS-VR

SUMMARY OF METHODOLOGY – REFER TO COMPREHENSIVE MANUAL FOR DETAILED INFORMATION

Step	Description	Table	Remarks
1	**Consequence Rating Range**	1	Each agency defines the range of consequence values. These values are used to modify Table 1 to agency needs.
2	Benefits of project or facility	-	Define all project benefits
3	**Project and Asset Consequences (C)**	1	Assign the project a C value. Develop a list of assets. Assign individual assets C values, using numeric values from 1-10. Determine which assets are critical.
4	**Vulnerability (V)** of individual dam structures and asset	4	Define the vulnerability of each identified dam structure and critical asset, using numeric values from 1-10
5	Essential Elements of information (EEI) and Prioritized Intelligence Requirements (PIR)	-	Develop a list of questions for a Threat Specialist to quantify the Threat in the area. Define actions needed to compromise assets.
6	**Probability of Loss (L)** of each asset	3	Determine the Probability of loss for each critical asset, using numeric values from 1-10.

DAMS-VR

Step	Description	Table	Remarks
7	**Loss Factor Rating (LF)**	-	**LF = (V x L)** for each critical asset.
8	**Priority Rating of Critical Assets**	4 & 5	Determine asset Priority Rating: Highly Probable, Probable, Moderately Probable, Improbable, or Extremely Improbable. Drop assets with ratings of Improbable and Extremely Improbable.
9	**Threat (T)** rating for individual Critical Asset	**6**	Determine a Threat value rating (1-10) for each Critical Asset.
10	**Security Effectiveness (S)** of individual Critical Assets	7	Determine a security value rating (1-10) for each Critical Asset.
11	**Asset Security Risk (ASR)** of individual Critical Assets	-	**ASR = C x (V + L + T + S)**
12-14	**Evaluate ASRs** and other data	-	Evaluate data; make recommendations to reduce risks; obtain preliminary cost estimates; prepare final report.

RAM-D/T - Risk Assessment Methodology for Dams & Electric Transmission Systems

Developed for the:

Interagency Forum for Infrastructure Protection (IFIP)

by:

Sandia National Laboratories

Albuquerque, NM

Robin Charlwood &
Rudy Matalucci

RAM-D/T - Risk Assessment Methodology

- Risk Equation $R = P_A * C * (1 – P_E)$
  - P_A = Likelihood of attack
  - C = Consequences of the loss from the attack
  - P_E = System Security effectiveness
  - $(1 – P_E)$ = Vulnerability (Likelihood that security system is not effective against an attack)
  - R = Risk associated with an adversary attack

Proprietary Information – Available under License only

RAM-D/T - Risk Assessment Methodology

- RAM-D/T addresses these items by a very systematic and fully documented process:
  - Screening events, consequences
  - Planning, develop fault-tree, threat estimates, consequences, assign priorities
  - Site survey, detection, delay, response
  - Analysis of “Adversary Sequence Diagrams”, system effectiveness, calculate risks
  - Risk Reduction, “Design Basis Threat”
  - Upgrade evaluation, cost, operation, schedule, public opinion
  - Final Report

RAMCAP – Dams Sector Risk Assessment Methodology

- Effort lead by U.S. Dept. of Homeland Security in coordination with government agencies (Corps of Engineers, Reclamation, FERC) and private dam owners.
  - Risk = R(Threat, Vulnerability, Consequences)
  - Methodology focused on facilitating comparison of results (across different owners) to enable rigorous national prioritization.
  - Comprehensive suite of attack scenarios considered as standard baseline for conditional risk analysis.
    - Conditional Risk = Rc(Vulnerability, Consequence)

RAMCAP – Dams Sector Risk Assessment Methodology (Cont)

- Methodology includes a consequence-based screening:
  - Consequences include:
    - Public health & Safety (Population at Risk)
    - Economic Impacts (Direct & Indirect Losses)
    - Impacts on Government & Mission Criticality
    - Psychological/Societal Impacts

- Conditional risk assessment allows identification of attack scenarios of highest concern.
- For risk assessment calculations, Loss of Life is used instead of Population at Risk.
- National effort still under development.