INSTITUTE FOR DEFENSE ANALYSES

An Integrated Approach for Physical and Cyber Security Risk Assessment: The U.S. Army Corps of Engineers Common Risk Model for Dams

Yazmin Seda-Sanabria
James D. Morgeson
Jason A. Dechant

July 2016
Approved for public release;
distribution is unlimited.
IDA Paper NS P-8092
Log: H 16-000878

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Project BA-6-3075, "Extending the Common Risk Model for Dams (CRM-D) Methodology," for the Director, Cost Assessment and Program Evaluation, Office of Secretary of Defense and the U.S. Army Corps of Engineers (USACE), Office of Homeland Security. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

The authors wish to thank Kevin Burns and the Editor, Dana Coppola for their work on this publication.

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper NS P-8092

An Integrated Approach for Physical and Cyber Security Risk Assessment: The U.S. Army Corps of Engineers Common Risk Model for Dams

Yazmin Seda-Sanabria
James D. Morgeson
Jason A. Dechant

This page is intentionally blank.

An Integrated Approach for Physical and Cyber Security Risk Assessment: The U.S. Army Corps of Engineers Common Risk Model for Dams

Yazmin Seda-Sanabria[1]
James D. Morgeson[2]
Jason A. Dechant, PhD[3]

I. ABSTRACT

The Common Risk Model for Dams (CRM-D), developed by the U.S. Army Corps of Engineers (USACE) in collaboration with the Institute for Defense Analyses (IDA) and the U.S. Department of Homeland Security (DHS), is a consistent, mathematically rigorous, and easy to implement method for security risk assessment of dams, navigation locks, hydropower projects, and appurtenant structures. The methodology provides a systematic approach for independently evaluating physical and cyber security risks across a portfolio of dams, and informing decisions on how to mitigate those risks. The CRM-D can effectively quantify the benefits of implementing a particular risk-mitigation strategy and, consequently, enable return-on-investment analyses for multiple physical and cyber security risk-mitigation alternatives and facilitate their implementation across a portfolio of dams.

A cyber security risk model to facilitate high-level risk assessments of industrial control systems used to control dam critical functions is also being implemented.

II. INTRODUCTION

In 2005, the Institute for Defense Analyses (IDA) initiated the development of the Common Risk Model (CRM) for evaluating and comparing risks associated with the nation's critical infrastructure. This model incorporates commonly used risk metrics that are designed to be transparent, simple, and mathematically justifiable. The model also enables comparisons of risks to critical assets, both within and across critical infrastructure sectors.

A modified version of this model has been under development by IDA in collaboration with the USACE. The extended model—Common Risk Model for Dams (CRM-D)—takes into account the unique features of dams and navigation locks and provides a systematic approach for evaluating and comparing risks from terrorist threats across a large portfolio[4] [7].

At the most basic level, risk is estimated for an attack scenario, defined as (1) a specific adversary (e.g., a highly capable transnational terrorist group), (2) a specific target (e.g., the main impounding structure of a specific dam), and (3) a specific attack vector (e.g., a cargo van loaded with explosives). Risk is a function of three variables: threat (T), vulnerability (V), and consequences (C):

$$R = f(T, V, C) \tag{1}$$

The three variables are defined as follows: threat – the probability of a specific attack scenario being attempted by the adversary, given an attack on one of the targets in the portfolio under assessment (P(A)); vulnerability – the probability of defeating the target's defenses, given that the attack is attempted (P(S|A)); and consequences – the estimated loss in terms of human life or economic damage given that the target's defenses are defeated (C). Because of how CRM-D estimates these three variables, it is appropriate to calculate risk as their product:

$$R = P(A) \times P(S|A) \times C \tag{2}$$

---

[1] National Program Manager, Critical Infrastructure Protection and Resilience Program, Office of Homeland Security, U.S. Army Corps of Engineers, Headquarters, Washington, DC.

[2] Research Staff Member, Strategy Forces and Resources Division, Institute for Defense Analyses, Alexandria, VA.

[3] Research Staff Member, Strategy Forces and Resources Division, Institute for Defense Analyses, Alexandria, VA.

[4] A portfolio is a set of dam projects evaluated by a risk analyst.

CRM-D also defines "conditional risk" (R_C) as risk for the attack scenario, given that this scenario is chosen:

$$R_C = P(S|A) \times C^5 \quad (3)$$

The consequence and risk metrics currently considered in the CRM-D are loss of life and total economic impacts. The aggregation of risks for all attack scenarios under consideration is termed "portfolio risk." Minimizing portfolio risk subject to available resources is often the focus of risk managers.

III. BASIC CONCEPTS: THE COMMON RISK MODEL FOR DAMS

A conceptually simple model of layered defenses is used to evaluate the conditional risk of a given critical infrastructure target. As an example, Figure 1 represents the case of a target protected by three notional defensive layers.

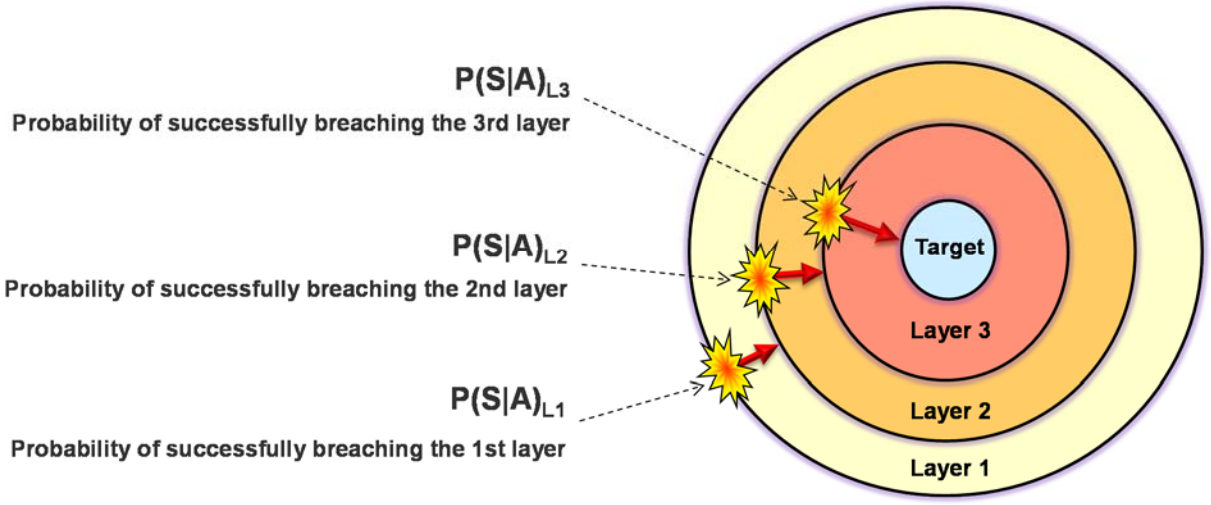

Figure 1. Conceptual Model of Layered Defenses

For the target to be successfully attacked, each defensive layer providing some form of protection needs to be successfully breached. For the case shown in Figure 1, the joint probability that a given attack, if attempted, will be successful in reaching the target (also known as the vulnerability or P(S|A)), can be determined using the following expression:[6]

$$P(S|A) = P(S|A)_{L1} \text{ x } P(S|A)_{L2} \text{ x } P(S|A)_{L3} \quad (4)$$

A team of subject matter experts (SMEs) estimated probabilities for each combination of attack vector and defensive configuration. As part of the CRM-D development, USACE defined a representative set of physical attack vectors to represent a wide spectrum of attacks that can be used to facilitate the comparison of vulnerability and conditional risk estimates across a large portfolio. These attack vectors,[7] which assume high-capability adversaries (well-trained attackers with significant access to resources), are listed in Table I and are arranged by categories known as *attack types*. The 28 attack vectors listed in Table I are a subset of the 32 total attack vectors defined by USACE for various adversary types.

[5] Note that the risk metric in Equation 2 is also conditional – on the attack within a portfolio under assessment. The "conditional risk" metric is further conditioned on the particular attack being chosen.

[6] The CRM-D model explicitly accounts for time delays in the attack due to the time it takes to breach layers and the time it takes to traverse interlayer distance. Also taken into account is attack vector degradation due to armed defenders. Since these are factors normally used in the estimation of conditional probabilities, CRM-D simplifies the calculation of conditional probabilities by assuming independence among the probability estimates except for those factors explicitly accounted for. See Morgeson et al., "Incorporating Uncertainties in Estimation of Vulnerabilities for Security Risk Assessments."

[7] The attack vectors used in CRM-D can be extended to include additional attack vectors that are identified over time.

Table I. Attack Vectors Considered for High-Capability Adversaries

ATTACK MODE	ATTACK TYPE	ATTACK VECTOR			
LAND	Vehicle–borne Improvised Explosive Device (VBIED)	Sedan	Cargo Van	Box Truck	Large Truck
	Assault Team	Single Attacker	Small-size Cell	Medium-size Cell	Large-size Cell
	Stand-off Weapon	Large-Caliber Rifle	Rocket-Propelled Grenade	Mortar	Man-portable Guided Missile
	Sabotage	Insider	Outsider	-	-
	Excavating Attack	Mechanical	Kinetic	-	-
WATER	Waterborne Improvised Explosive Device (WBIED)	Inflatable Boat	Small Boat	Large Boat	Barge
	Underwater Improvised Explosive Device	Surface Swimmer	Subsurface Swimmer	Modified Small Boat	Semi-submersible Boat
AIR	Impact	Helicopter	Small Airplane	Narrow-body Airliner	Wide-body Airliner

The probability that a specific attack vector would be successful in reaching a given target depends on the probability that each of the defensive layers encountered sequentially along the attack path is penetrated successfully. These individual layer probabilities, in turn, depend on the type of adversary, the attack vector chosen, and the strength of the defenses at that particular layer [5]. To illustrate the concept, assume that a given target T-1 is protected by three defensive layers (L_1, L_2, and L_3). For a given attack vector denoted as AV-1, the overall probability of success for the scenario defined by attack vector AV-1 and the target T-1 is the joint probability of penetrating all three layers successfully. For this scenario, Equation 4 can be written using the following notation:

$$P(S|A)_{Overall} = P(S|A)_{AV\text{-}1,\,L1} \times P(S|A)_{AV\text{-}1,\,L2} \times P(S|A)_{AV\text{-}1,\,L3} \quad (5)$$

Equation 6 is an example of the calculation in Equation 5 using notional estimates for the probabilities for each layer.

$$P(S|A)_{Overall} = 0.2 \times 0.7 \times 0.9 = 0.126 \quad (6)$$

As defined by Equation 3, conditional risk is the product of the probability of successful attack (given that the attack is attempted) multiplied by the corresponding consequences. For illustrative purposes, assume that the economic consequences of a successful attack on target T-1 is estimated to be \$1.0 million (M); therefore,

$$R_C = P(S|A) \times C = 0.126 \times \$1.0M = \$126{,}000 \quad (7)$$

R_C is the expected loss given a hypothetical attack on target T-1 protected by layers L_1, L_2, and L_3. Therefore, for every attack scenario (i.e., combination of an adversary type, a specific attack vector, and a given target), the CRM-D methodology provides a systematic approach to estimate conditional risk. Table II contains conditional risk calculations for a set of scenarios at a notional dam.

Table II. Conditional Risk for Selected Attack Scenarios for a Notional Dam

Attack Type	Attack Vector	Impoundment					Powerhouse (Control Center)					Powerhouse (Turbines and Generators)				
		Conseq.		$P(S\|A)_{FINAL}$	Conditional Risk (Life)	Conditional Risk (Econ. $M)	Conseq.		$P(S\|A)_{FINAL}$	Conditional Risk (Life)	Conditional Risk (Econ. $M)	Conseq.		$P(S\|A)_{FINAL}$	Conditional Risk (Life)	Conditional Risk (Econ. $M)
		Loss of Life	Economic Loss ($M)				Loss of Life	Economic Loss ($M)				Loss of Life	Economic Loss ($M)			
VBIED	Sedan	1	1	1.0	1	1	11	1	1.0	11	1	1	22	1.0	1	22
	Van	1	3	1.0	1	3	11	3	1.0	11	3	1	22	1.0	1	22
	Box Truck	1	3	1.0	1	3	11	3	1.0	11	3	1	44	1.0	1	44
	Large Truck	100	200	1.0	100	200	11	3	1.0	11	3	1	66	1.0	1	66
Assault Team	Single Attacker	1	0	0.51	1	0	11	3	0.58	6	2	1	44	0.58	1	25
	Small Cell	1	0	0.9	1	0	11	3	0.81	9	2	1	132	0.81	1	107
	Medium Cell	1	1	1.0	1	1	11	3	1.0	11	3	1	132	1.0	1	132
	Large Cell	1	1	1.0	1	1	11	3	1.0	11	3	1	132	1.0	1	132

Source: The data in Table 2 and associated graphics throughout this paper are drawn from Michael Keleher, Steven Walser, and Samuel Himel, The Common Risk Model for Dams Support System: A Prototype Analyst Tool (Alexandria, VA: Institute for Defense Analyses, IDA Paper P-5220). Values in the table are rounded.

IV. EXPOSURE: A DECISION METRIC

When estimating conditional risk, a dam with only a modest number of critical assets could have several hundred scenarios and, consequently, several hundred conditional risk estimates. A decision metric, defined as *exposure*, is used to facilitate the aggregation of conditional risk estimates across scenarios. A standard set of graphics and return-on-investment calculations based on exposure are introduced that summarize the current level of risk at a dam project, as well as the reduced level of risk if the set of recommended security upgrades are implemented.

A. Defining Exposure

Exposure is defined as human lives and economic value at risk due to an attack. It is calculated as the scaled sum of conditional risk estimates for any particular set of scenarios (or even a single scenario) being considered by the analyst. Intuitively, the number of human lives at risk from a single attack at a specified dam cannot exceed the maximum number of lives lost considering all scenarios at that dam. Consequently, exposure, measured in terms of lives lost, for any set of scenarios will never exceed the maximum possible lives lost from any individual scenario in the set. The analyst can use exposure to compare risks by attack type, by target, or for any useful set of scenarios. The results of this comparison can guide an analyst in determining the most effective set of security upgrades.

V. USING EXPOSURE TO DEVELOP RISK-MITIGATION OPTIONS

A risk-mitigation option (RMO) is the designation given to a package of security upgrades intended to reduce exposure at critical assets and components of a dam project. The upgrades consist of improvements or additions to the defensive layers of the project. Options are constrained in practice by command guidance, such as funding limitations or operational considerations.

The decision metric that will be used to evaluate potential RMOs is the net reduction in the exposure for the set of all scenarios considered at the project. Exposure for a dam in its current security configuration is denoted $RC'_{As\text{-}Is}$. It is calculated[8] using conditional risk estimates for each scenario based on the P(S|A) values for the current defensive configuration at each layer protecting the dam. RC'RMO denotes exposure for the dam after implementing the proposed RMO. It is calculated using conditional risk estimates for each scenario based on revised P(S|A) values resulting from the proposed defensive configurations.

Exposure was introduced to help the analyst use conditional risk estimates to develop RMOs that effectively reduce risk. It scales all conditional risks to prevent their sum from exceeding the maximum consequences from the most consequential single attack. Exposure, calculated by summing scaled conditional risk values over different sets of scenarios, is particularly helpful in answering two questions from the dam owner/operator perspective:

1) Which targets are the most exposed?
2) Which attack types have the highest risk of exposure?

The first question is addressed by calculating exposure for each asset at the dam. That is, calculate the sum of scaled conditional risk estimates for all scenarios involving a particular asset. Similarly, the second question is addressed by calculating exposure for each attack type. That is, calculate the sum of scaled conditional risk estimates over each scenario involving a particular attack type. In the next section, graphics are introduced that help the analyst answer these two questions.

A. Understanding the Effectiveness of RMO Options

Each scenario contributes to the overall exposure at a dam project. In order for an analyst to recommend security upgrades that efficiently reduce that level of exposure, it would be helpful to know which scenarios contribute the most to the overall level of exposure. As previously mentioned, this can be analyzed by asset or by attack type. Pie charts are an intuitive way to display this information.

Figure 2 and Figure 3 show how exposure is distributed over assets and attack vectors for current defenses at a notional dam. Charts such as these inform the analyst during the process of building RMOs. $R_C'_{As\text{-}Is}$ is calculated for the set of all scenarios; each wedge in the pie charts represents the percentage of that total that is contributed by the set of scenarios that involve only the asset (or attack type) indicated.

Figure 2 displays relevant information to determine which targets are the most exposed in terms of loss of life. As shown, more than half of all exposure is contributed by scenarios involving only two assets—the visitor center and the main impounding structure. This information provides insight to the risk analyst in making a determination on where security upgrades are best placed at a dam project to reduce exposure.

[8] Exposure is defined and calculated, both in terms of human lives and economic value. The calculations for human lives and economic value are always done separately.

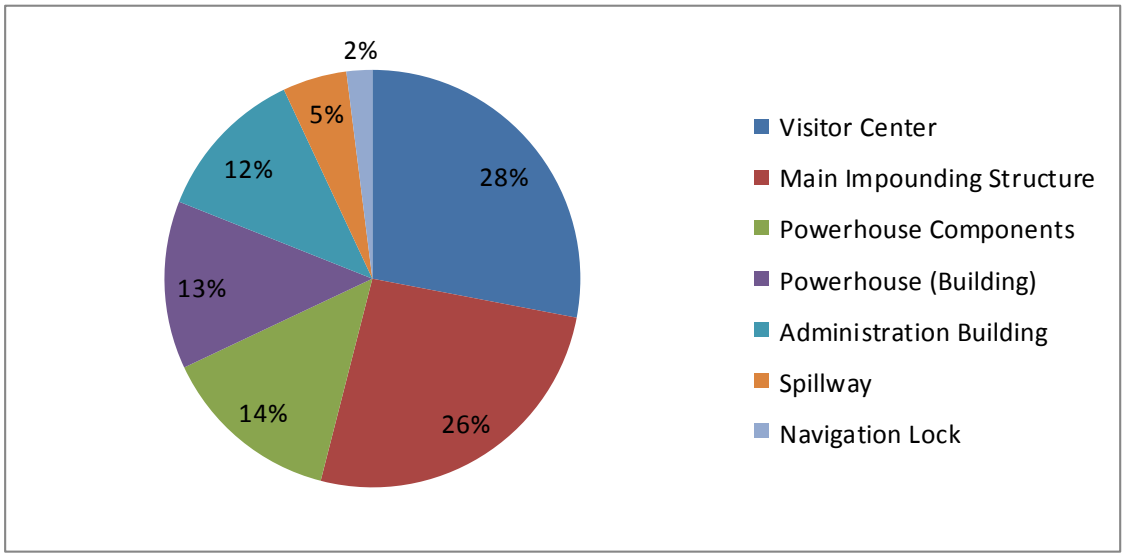

Figure 2. Distribution of Loss-of-Life Exposure Over Assets for "As-Is" Defenses

A similar analysis can be conducted by attack type. Figure 3 shows information on which attack vectors currently cause the most exposure. It shows that roughly three quarters of total exposure at the project is attributed to scenarios involving vehicle-borne improvised explosive devices (VBIEDs) and assault teams. An analyst can readily surmise that protecting against land-based attacks is more likely to lower overall exposure than protecting against waterborne attacks.

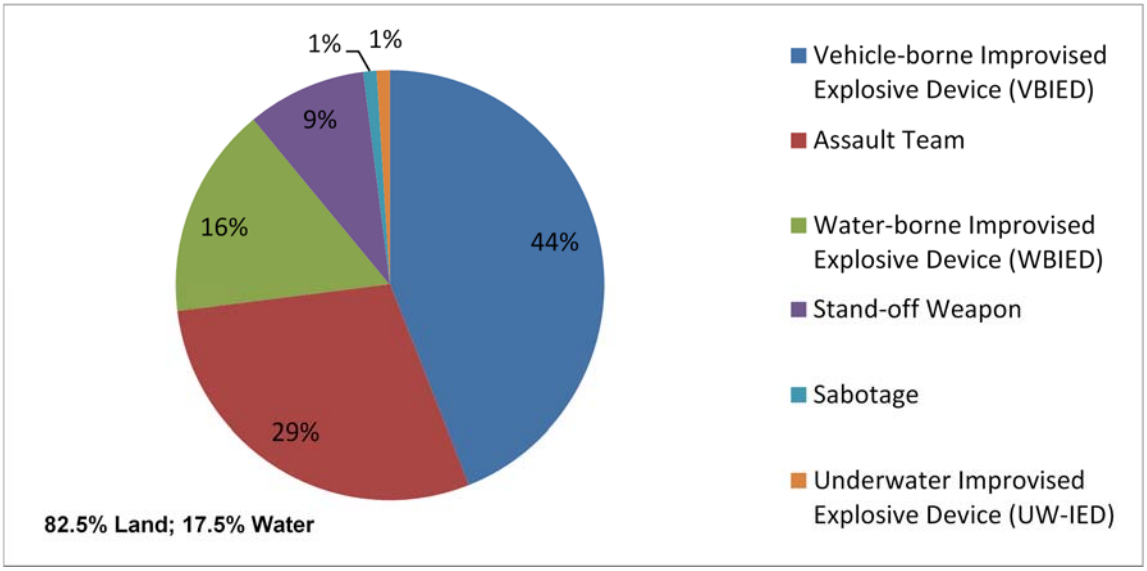

Figure 3. Distribution of Loss-of-Life Exposure Over Attack Vector Types for "As-Is" Defenses

B. Evaluating Alternative RMOs

For a given RMO, it is important to quantify the reduction in exposure that would be achieved if the proposed RMO is implemented. Figure 4 depicts a notional example where three separate estimates of loss of life exposure are shown for three different security conditions at a given dam: (1) no effective defenses present, (2) existing security configuration, and; (3) proposed security configuration based on implementation of the RMO.

The left bar (RED), denoted as $R_C'_{UNDEFENDED}$, represents the level of exposure if there were no effective defenses at the dam; that is, the vulnerability, or P(S|A), for every scenario equals 1.0. Mathematically, this means that R_C equals the associated consequences for every scenario. In this case, R_C' equals the maximum consequences that can be achieved for all scenarios being considered.

The middle bar (BLUE) represents the level of exposure associated with the current state of defenses. The example in Figure 4 shows that the current security configuration provides a 21 percent reduction in exposure, as compared to an undefended project.

The right bar (GREEN) represents the level of exposure if the proposed RMO was implemented. Adding these proposed security enhancements would result in a 17 percent reduction in the level of loss-of-life exposure, as compared to the current security configuration.

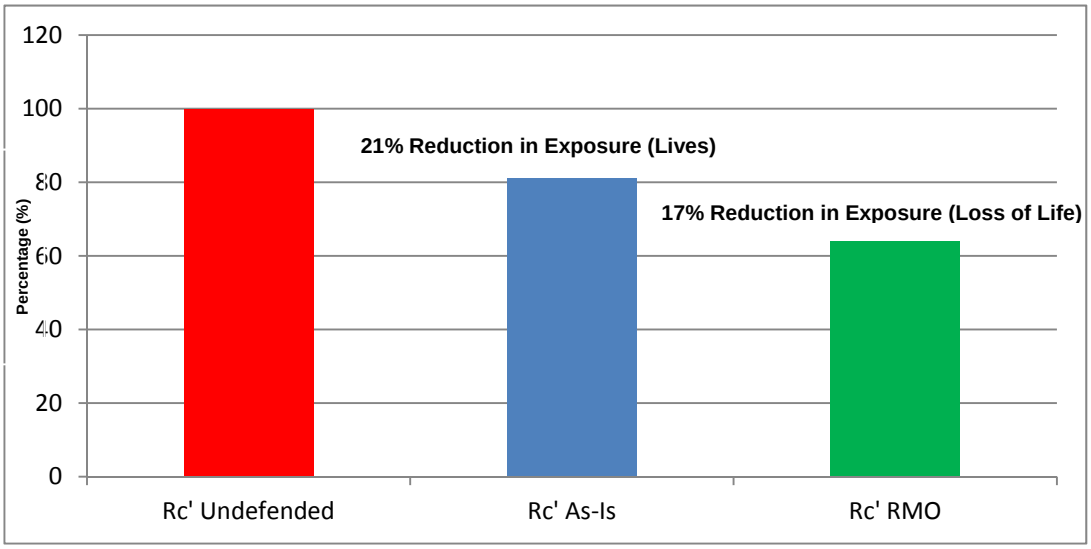

Figure 4. Reduction in Loss-of-Life Exposure for RMO

Exposure is an intuitive concept that provides risk analysts with an easy-to-calculate method for synthesizing conditional risk calculations across multiple scenarios. The data provided by this new metric can be presented to decision makers via graphical displays that are informative and easy to comprehend.

VI. ESTIMATING THREAT: P(A)

As noted previously, risk is a function of threat, vulnerability, and consequences. Preceding sections address the estimation of vulnerability and consequences, but estimation of threat to a dam project is an important part of risk assessment. Because attempted or even planned attacks on the U.S. infrastructure are, fortunately, rather rare, there is a lack of historical data to quantify threat for attack scenarios in terms of the historical frequency of their occurrence, as would often be done with natural hazards. Thus, in order to quantify risk as an expected loss, threat needs to be estimated as a *subjective probability*, a formally quantified judgment by subject-matter experts (SMEs) about the relative likelihood of each attack scenario.

The CRM-D methodology incorporates a terrorist decision model (formally known as the *Probabilistic Adversary Decision Model*), which can be used to systematically estimate the relative likelihood of potential attack scenarios for any given portfolio of dams. The terrorist decision model is derived from information elicited from terrorism experts and intelligence analysts. Once the model has been developed using expert elicitation, it can be used to estimate threat for any number of attack scenarios and to accommodate additional scenarios without conducting new elicitations. The approach, which is based on the conjoint (trade-off) analysis methodology used frequently in market research, constitutes a unique contribution to the methods of eliciting expert uncertainty and aggregating expert opinions. The model quantifies the reduction of relative threat as a result of a particular risk mitigation strategy and, consequently, enables return-on-investment analyses for multiple risk mitigation alternatives.

A. Modeling Adaptive Threats

Modeling threat from goal-oriented, adaptive adversaries is fundamentally different from modeling potential hazards associated with forces of nature. Adversaries *evaluate* potential attacks based on criteria that are important to them and then *choose* the attack that accords best with their objectives. When the adversary's decision criteria change, their choice may change as well. Unlike consequence or vulnerability estimates, a threat estimate for an attack scenario depends not only on the characteristics of that scenario, but also on the characteristics of all attack scenarios from which the adversary is choosing.

To account for these concepts, the CRM-D includes a Probabilistic Adversary Decision Model (PADM), which is composed of two sub-models: the *Adversary Value Model* (AVM) and the *Attack Choice Model* (ACM). The decision model is probabilistic because no aspect of the adversary's future decision process can be known with certainty.

Adversary Value Model. This model quantifies expert judgment about how adversaries evaluate the relative attractiveness of attack scenarios based on the scenarios' characteristics that the adversary is likely to take into account. These features, related to the adversary capabilities and intent, reflect the various expected benefits, costs, and risks associated with each attack scenario. The adversary value model also quantifies the underlying uncertainty about the value system, which stems from the differences of opinion among experts and the uncertainty of each individual expert about the attacker's value system.

To model the attack scenario evaluation process followed by an adversary, it is first necessary to identify the adversarial goals driving the selection of a particular attack scenario. For the type of adversary under consideration (highly capable, transnational terrorist organization), this was conducted through literature review and interviews with selected groups of terrorism experts from various government and research organizations.

Based on the assumed goals, the following variables were identified as the controlling factors influencing the attack scenario evaluation process from the adversary's perspective:

- Adversary's perception of the probability of successfully defeating the national and local defensive layers;
- Adversary's perception of the probability of successfully defeating the target defensive layers, given success against the national and local defenses;
- Adversary's perception of the expected level of consequences in terms of the loss of life resulting from a successful attack;
- Adversary's perception of the expected level of consequences in terms of the economic impacts resulting from a successful attack.

A comprehensive expert elicitation used to develop the PADM was conducted with the participation of representatives from multiple federal agencies, owners and operators, state fusion centers, and other state agencies responsible for law enforcement and public safety. In the main elicitation task, each SME was presented with one or two dozen different sets of four hypothetical attack alternatives. For each set of alternatives, each expert was asked to provide the probability that each of the alternatives in the set would be chosen by adversaries, given that one of them is chosen. Eliciting probabilities provides a way to incorporate each SME's uncertainty. Figure 5 shows an example of one of the sets of hypothetical attack alternatives used in the elicitation.

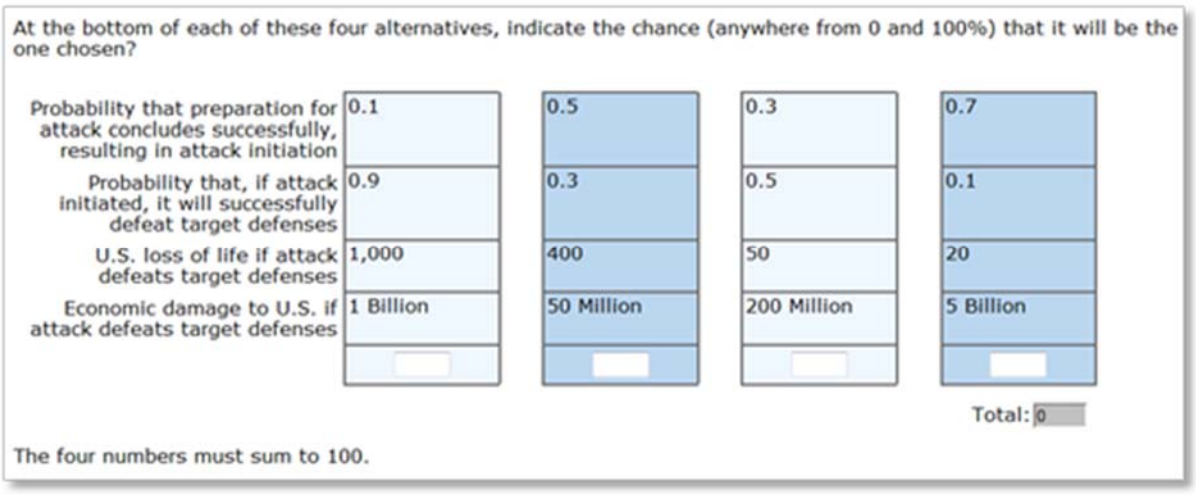

Figure 5. Example of a Set of Hypothetical Attack Alternatives

Attack Choice Model. The attack choice model uses the estimated adversary value system to calculate P(A) for any set of attack scenarios and to perform return on investment (ROI) analyses for risk-mitigation alternatives. To enable P(A) calculation, attack scenarios in the portfolio need to be formulated in terms that the adversary value model can accommodate. This involves using the CRM-D consequence and vulnerability models to estimate the values for loss of life, total economic impacts, and the probabilities of defeating the national/local and target defenses for every scenario in the portfolio. These variables are used as proxies for the adversary perceptions of these variables. The model then uses the estimated adversary value function and the uncertainty around it to simulate the possible utility values for a set of attack scenarios. The CRM-D assumption is that the adversary selects the attack scenario perceived to have the highest value, and so P(A) for an attack scenario is calculated as the fraction of the simulations, in which the scenario has the highest value in the set.[9]

Because CRM-D models adversaries as adaptive decision makers, it is important to note that some risk-mitigation investments may decrease P(A) for some scenarios while causing an increase for other scenarios.[10] Therefore, it is theoretically possible for an investment aimed at risk mitigation to actually increase portfolio risk if the threat shifts to attack scenarios that pose more risk. Risk managers should be mindful of the complex interactions associated with the target selection process employed by adaptive adversaries.

B. Estimation of Total Risk

Figure 6 demonstrates how risk estimates can be used by decision makers. Each dot in the figure represents a particular scenario from a portfolio of dams. The vertical axis represents the product of P(A) and P(S|A), and the horizontal axis represents the economic consequences (notice that the targets are indexed by letters, and the attack vectors by numbers). Total risk is estimated in terms of economic consequences by multiplying the values of each coordinate set.

The figure depicts iso-curves representing thresholds of total risk. As an example, points above the red line represent dams where risk is greater than $50M. Decision makers can use this information to identify dams where risk is greatest, representing a priority for implementation of risk mitigation investments.

[9] If the adversary believes that risk mitigation might involve deception or randomization, they might not necessarily choose a scenario that is perceived to have the highest value.

[10] Because P(A) is conditional on attack within a portfolio, deterrence is not modeled – in response to risk mitigation, the P(A) can only shift among the scenarios, and the sum of P(A) will always be no less than 1. Future work on the AVM elicitation will enable estimating the deterrence effect of investments.

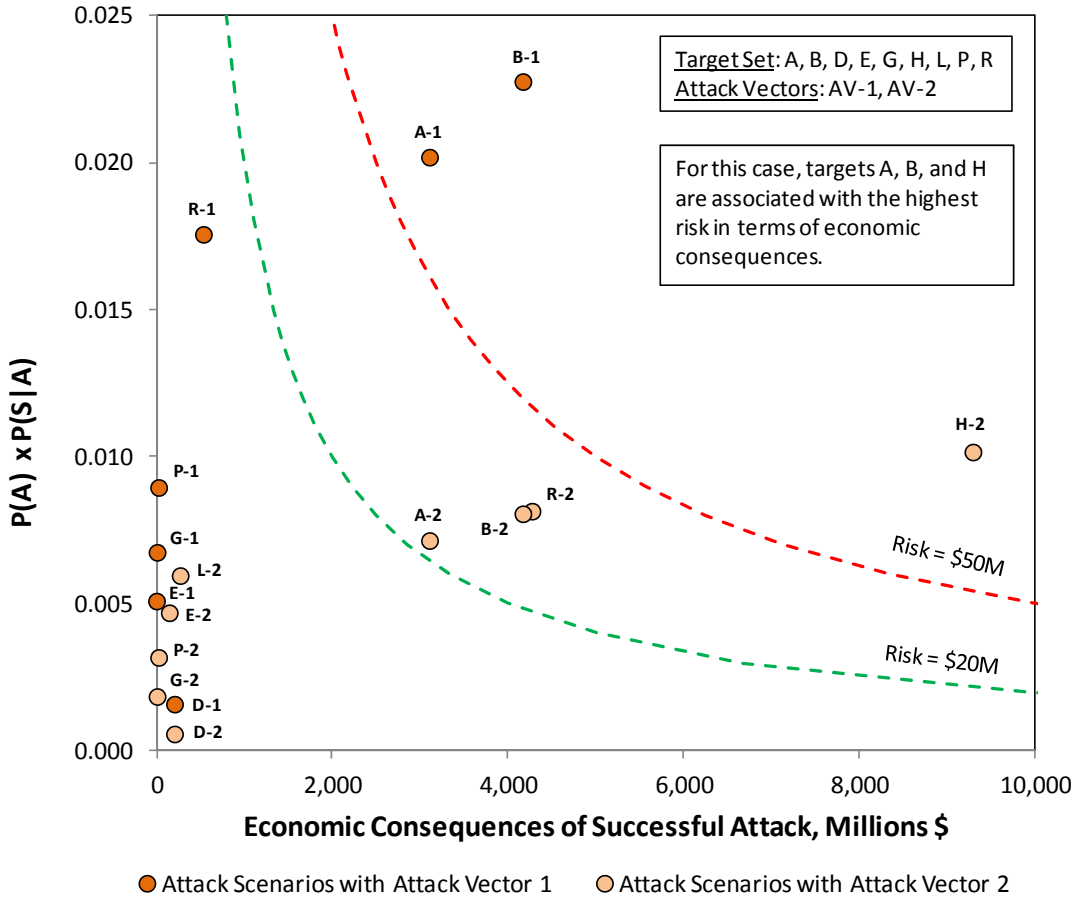

Figure 6. Total Risk Estimation in Terms of Economic Consequences

Previously, it was shown how exposure has been used to aggregate risk across scenarios and thus to aid in the development and evaluation of RMOs. Estimates of P(A) for each scenario can also be used to synthesize risk across scenarios. Thus, decision makers have two methods at their disposal for evaluating various RMOs. However, exposure is the method currently implemented by USACE.

VII. CYBER SECURITY RISK MODEL

The National Infrastructure Protection Plan (NIPP, 2013) sets forth goals for a national, coordinated effort to strengthen the security and resilience of our nation's critical infrastructure against human, physical, and cyber threats. It outlines a coordinated risk-management framework to secure the cyber elements of critical infrastructure in an integrated fashion with physical security, rather than as a separate consideration.

To achieve this goal, USACE has expanded the CRM-D to incorporate a risk model focused on cyber-attack scenarios on industrial control systems (ICS) controlling critical dam functions. This model enables the implementation of high-level cyber-risk assessments, and assists in the identification of those ICS where stronger cyber-security measures should be implemented in order to reduce risks to an acceptable level.

A. Estimating Vulnerability

Cyber vulnerability is defined as the probability of defeating cyber defenses, given a cyber attack. For the target to be successfully attacked, the cyber-defensive configuration would need to be successfully breached.

To assess vulnerability, ICS configurations have been classified into four system architecture categories representative of USACE dams, as follows:

1) Platform Information Technology (PIT) System Restricted Interconnection – refers to a system connected to a project owned by an entity external to USACE.
2) PIT System Closed-Restricted – a set of multiple interconnected systems capable of enabling remote operations,
3) PIT System – a system with no external connections,
4) PIT Product –the simplest control system with minimal computing resources.

Similarly, a number of cyber defense packages with increasingly strong levels of cyber protection have been defined (e.g., the higher the designation, the stronger the defense package). The CRM-D considers a total of six different cyber defense package levels, ranging from the fewest or most ineffective controls (Cyber Defense Package 0) to the most stringent controls (Cyber Defense Package 5). These cyber defense packages are comprised of physical defenses, personnel measures, and cyber controls. Physical defenses may include elements such as gates, access controls, surveillance systems, etc. Similarly, typical personnel measures include background checks and cyber security training, while some sample cyber controls involve computer access controls and system monitoring.

Table III shows qualitative assessments of cyber vulnerability, or the probability that a given cyber attack, if attempted, will be successful in defeating cyber defenses (also known as the vulnerability or P(S|A)). These estimates were developed using SME expert elicitation considering a high-capability adversary. A cyber vulnerability rating can be determined by considering the system architecture in place and its corresponding cyber defense package level.

Table III. Cyber Vulnerability Rating for High-End Adversaries

CYBER DEFENSE PACKAGE	SYSTEM ARCHITECTURE			
	PIT SYSTEM RESTRICTED INTER-CONNECTION	PIT SYSTEM CLOSED RESTRICTED	PIT SUBSYSTEM	PIT PRODUCT
DEFENSE PACKAGE 5	Very Low			
DEFENSE PACKAGE 4	Low	Very Low	Extremely Low	
DEFENSE PACKAGE 3	Moderate	Low	Very Low	
DEFENSE PACKAGE 2	High	Moderate	Low	Extremely Low
DEFENSE PACKAGE 1	Very High	High	Moderate	Low
DEFENSE PACKAGE 0	Extremely High	Extremely High	Extremely High	Extremely High

B. Estimating Consequences

Just as in the case of physical attacks, consequences associated with cyberattacks are also estimated in terms of loss of lives and economic damages. For each dam critical function, potential damages are estimated by considering worst reasonable case conditions. A representative[11] worst reasonable case scenario for each major dam function is characterized as follows:

- Flood Risk Management. Flood control (spillway) gates connected to an ICS are assumed to be compromised, but not destroyed or damaged. Gate operation mechanisms may be damaged. Manual override/control is assumed possible for all ICS-controlled gates.
- Hydropower. All turbines and power generators that are connected to the ICS and an external connection are assumed to be destroyed. Serial connections (e.g., analog signals sent to and/or from regional power administrations) are not counted as external communications systems. If no external connection is present, the generators controlled by the ICS are assumed to be disabled for the duration of the cyber attack. All other hydropower components connected to ICS are assumed disabled for the duration of the event (i.e., time to restore full operational capabilities).
- Navigation. All navigation lock (miter) gates connected to an ICS are assumed to be damaged.
- Water Supply. All water supply-related components connected to an ICS are assumed to be compromised, but not destroyed or damaged. All saltwater intrusion gates connected to an ICS are assumed to be damaged. Additionally, any loss of pool due to a successful cyber attack on any other critical interdependent function (i.e., flood risk management, hydropower, or navigation) may impact the project's ability to supply water normally.

Once the potential damages for each function are estimated, the overall worst condition resulting from the evaluation of all critical dam functions is determined and used to assign a consequence rating based on loss of life (Table IV) and total economic loss (Table V), which range from the lowest (Level 1) to the highest (Level 5) impacts.

Table IV. Consequence Rating (Loss of Life)

LOSS OF LIFE CONSEQUENCE RATING				
Level 1	Level 2	Level 3	Level 4	Level 5
0	0 < LOL ≤ 50	50 < LOL ≤ 100	100 < LOL ≤ 200	> 200

Table V. Consequence Rating (Economic Loss)

ECONOMIC LOSS CONSEQUENCE RATING				
Level 1	Level 2	Level 3	Level 4	Level 5
< $1.0M	$1.0M < X ≤ $25.0M	$25.0M < X ≤ $50.0M	$50.0M < X ≤ $100.0M	> $100.0M

C. Estimating Risk

Table VI shows how to estimate cyber risk for ICS associated with dams. By combining the vulnerability rating with the corresponding consequence rating (either loss of life or economic loss), a qualitative risk rating associated with each combination of vulnerability and consequence ratings is assigned, ranging from "Very Low" to "Very High."

[11] The actual "worst reasonable case scenario" for each critical function is dependent on individual dam cyber-configurations and subject to change based on the outcomes of actual cyber attacks, identification of new vulnerabilities and new threats, and intelligence.

Table VI. Industrial Control Systems Cyber Risk Rating

VULNERABILITY RATING	CONSEQUENCE RATING				
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
EXTREMELY HIGH	Very Low	Low	High	Very High	Very High
VERY HIGH	Very Low	Low	Moderate	Very High	Very High
HIGH	Very Low	Low	Moderate	High	Very High
MODERATE	Very Low	Low	Moderate	Moderate	High
LOW	Very Low	Low	Low	Low	Moderate
VERY LOW	Very Low	Very Low	Low	Low	Low
EXTREMELY LOW	Very Low	Very Low	Very Low	Low	Low

VIII. CONCLUSION

The CRM-D is a consistent, mathematically rigorous, and easy to implement method for security risk assessment of dams, navigation locks, hydropower projects, and appurtenant structures. This methodology, the implementation of which represents collaborative efforts between USACE and DHS, provides a systematic approach for evaluating and comparing security risks across a large portfolio.

Risk is calculated for attack scenarios as a function of consequences, vulnerability, and threat. Vulnerability estimates are elicited as probabilities of successful attacks by specific adversary types using reference attack vectors against generic security configurations. The elicited estimates can then be used to estimate the vulnerability of a target protected by any combination of the generic security configurations against any of the reference attack vectors for the adversary groups under consideration. The CRM-D also incorporates a probabilistic adversary decision model to estimate the probability of each attack scenario in the set, given that one of the scenarios in the set is attempted. The CRM-D can effectively quantify the benefits of implementing a particular risk-mitigation strategy and, consequently, enable return-on-investment analyses for multiple risk mitigation alternatives across a large portfolio.

A cyber security risk model for the evaluation of security risk on ICS controlling critical dam functions is now implemented as part of CRM-D. A risk rating scheme is used to assign a risk level and identify ICS where stronger cyber-security measures should be implemented in order to reduce risks to an acceptable level.

The elements of CRM-D provide risk analysts with a suite of rigorous tools for estimating physical and cyber security risks across a portfolio of dams. The results from a CRM-D risk assessment can be used to inform investment decisions to mitigate those risks and enhance the security posture at our nation’s critical infrastructure against potential adversaries.

IX. ACKNOWLEDGEMENTS

This research was supported by the U.S. Army Corps of Engineers, Headquarters, Office of Homeland Security, Critical Infrastructure Protection and Resilience Program. We would like to express our sincere gratitude to our colleagues from the U.S. Department of Homeland Security, in particular Dr. Enrique E. Matheu, Office of Infrastructure Protection, Sector Outreach and Partnership Division, who provided invaluable insight and technical expertise that greatly assisted in the development of this methodology. We are indebted to the research staff at the Institute for Defense Analyses, Strategy Forces and Resources Division, for their technical contributions, unique knowledge, and wealth of expertise, in particular Dr. M. Anthony Fainberg, Anthony C. Hermes, Dr. Victor A. Utgoff, Dr. Yevgeniy Kirpichevsky, Michael J. Keleher, Dr. Kevin E. Burns, and Dr. Kevin F. McCrohan, Finally, we want to share our appreciation of Strati Oktay and Corey C. Hade, Battelle Memorial Institute, Critical Infrastructure Security and Resilience Division, for their significant contributions to the implementation and operationalizing of this methodology.

X. REFERENCES

[1] Burns, K.J., Dechant, J.A., Hermes, A.C., Keleher, M.J, Kirpichevsky, Y., and Morgeson, J.D. 2016. "The Common Risk Model for Dams Volume I: Methodology." IDA Paper P-5295. Alexandria, VA: Institute for Defense Analyses.

[2] Burns, K.J., Morgeson, J.D., Dechant, J.A., Seda-Sanabria, Y., and Matheu, E.E. 2015. "Exposure: A New Decision Metric for Selecting Effective Sets of Security Upgrades." IDA NS-D-5324. Alexandria, VA: Institute for Defense Analyses.

[3] Kirpichevsky, Y., Matheu, E.E., and Seda-Sanabria, Y. 2012. "Modeling Adaptive Threats: Incorporating A Terrorist Decision Model Into Security Risk Assessments." In *Proceedings of the 32th USSD Annual Meeting and Conference*, New Orleans, LA, April.

[4] Kirpichevsky, Y., Morgeson, J.D., Seda-Sanabria, Y., Matheu, E.E., Fainberg, M.A., Dechant, J.A., and Utgoff, V. 2012. "Security Risk Assessments Using the Common Risk Model for Dams (CRM-D): Portfolio Risk Analysis Incorporating Threat Modeling." In *Proceedings Dam Safety 2012 Conference – Fifth Annual National Dam Security Forum*, Denver, CO. September.

[5] Morgeson, J.D., Seda-Sanabria, Y., Matheu, E.E., Keleher, M.J. 2013. "Incorporating Uncertainties in Estimation of Vulnerabilities for Security Risk Assessments." *In Proceedings 33rd USSD Annual Meeting and Conference*, Phoenix, Arizona, February 11–15.

[6] National Research Council. 2010. *Review of the Department of Homeland Security's Approach to Risk Analysis.* Washington, DC: The National Academies Press.

[7] Seda-Sanabria, Y., Matheu, E.E., and Fainberg, M.A. 2011. "Security Risk Assessment of Dams and Navigation Locks," *3rd International Forum on Risk Analysis, Dam Safety, Dam Security, and Critical Infrastructure Management*, Valencia, Spain, October 17-18.

[8] Seda-Sanabria, Y., Matheu, E.E., Morgeson, J.D., Kirpichevsky, Y., Fainberg, M.A., Dechant, J.A., and Utgoff, V. 2013. "The Common Risk Model for Dams: A Portfolio Approach to Security Risk Assessments", *International Journal on Hydropower and Dams* (special ICOLD Issue: Hydropower & Dams in North America), pp. 78-82.

[9] U.S. Department of Homeland Security. 2013. *National Infrastructure Protection Plan*: *Partnering for Critical Infrastructure Security and Resilience.*
https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

[10] U.S. Government Accountability Office. 2005. *Further Refinements Needed To Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.* GAO-06-91. http://www.gao.gov/products/GAO-06-91.

YAZMIN SEDA-SANABRIA

Yazmin Seda-Sanabria serves as the National Program Manager of the Office of Homeland Security's Critical Infrastructure Protection and Resilience Program Office of Homeland Security at the U.S. Army Corps of Engineers, Headquarters. In this role, she provides oversight for program development, execution, and implementation of risk management strategies for enhancing the security and resilience of USACE's Civil Works critical infrastructure projects.

In 1994, Ms. Seda-Sanabria joined the U.S. Army Engineer Waterways Experiment Station – now U.S. Army Engineer Research and Development Center (ERDC) – as a research structural engineer in the Geosciences and Structures Division, Geotechnical and Structures Laboratory. While at ERDC, she was involved in multiple research and development programs related to analysis and design of Civil Works water resource development projects, as well as military engineering bridge assessment technologies. She joined USACE Headquarters in 2006 as the Executive Direction and Management, General Expenses Program Manager in the Civil Works Program Integration Division. In 2007, Ms. Seda-Sanabria joined the Office of Homeland Security in her current position.

Ms. Seda-Sanabria holds a Bachelor's degree and Master's degree in Civil Engineering from the University of Puerto Rico at Mayagüez, and a second Master's degree in Engineering Mechanics from Mississippi State University. In 1998, she received the American Society of Civil Engineers' Young Government Civil Engineer National Award, in recognition of her public and professional service achievements. In 2002, she received the Women of Color Government and Defense Award for Technical Innovation, in recognition for her efforts leading to the development and implementation of innovative technologies for rapid load capacity assessment of bridges. In 2009, she received the Hispanic Engineer National Achievement Award, Civil Engineering distinction for her contribution to critical infrastructure protection. She has authored over 40 publications, including peer-reviewed journal and conference papers, invited articles, and technical reports. She is also a member of various professional engineering organizations, including the American Society of Civil Engineers Engineering Mechanics Institute, the Association of State Dam Safety Officials, the United States Society of Dams, and the Sigma Xi Research Society.

This page is intentionally blank.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
xx-07-16	Final	

4. TITLE AND SUBTITLE

An Integrated Approach for Physical and Cyber Security Risk Assessment: The U.S. Army Corps of Engineers Common Risk Model for Dams

5a. CONTRACT NO.

HQ0034-14-D-0001

5b. GRANT NO.

5c. PROGRAM ELEMENT NO(S).

6. AUTHOR(S)

Yazmin Seda-Sanabria
James D. Morgeson
Jason A. Dechant

5d. PROJECT NO.

5e. TASK NO.

BA-6-3075

5f. WORK UNIT NO.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NO.

IDA Paper NS P-8092
H 16-000878

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Corps of Engineers
Critical Infrastructure Protection & Resilience (CIPR) Program
Office of Homeland Security
U.S. Army Corps of Engineers, Headquarters
441 G Street NW
Washington, DC 20314-1000

10. SPONSOR'S / MONITOR'S ACRONYM(S)

USACE

11. SPONSOR'S / MONITOR'S REPORT NO(S).

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Common Risk Model for Dams (CRM-D), developed by the U.S. Army Corps of Engineers (USACE) in collaboration with the Institute for Defense Analyses (IDA) and the U.S. Department of Homeland Security (DHS), is a consistent, mathematically rigorous, and easy to implement method for security risk assessment of dams, navigation locks, hydropower projects, and appurtenant structures. The methodology provides a systematic approach for independently evaluating physical and cyber security risks across a portfolio of dams, and informing decisions on how to mitigate those risks. The CRM-D can effectively quantify the benefits of implementing a particular risk-mitigation strategy and, consequently, enable return-on-investment analyses for multiple physical and cyber security risk-mitigation alternatives and facilitate their implementation across a portfolio of dams.

A cyber security risk model to facilitate high-level risk assessments of industrial control systems used to control dam critical functions is also being implemented.

15. SUBJECT TERMS

Common Risk Model for Dams, Risk, Exposure, Dams Sector

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NO. OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Yazmin Seda-Sanabria
U	U	U	U	24	19b. TELEPHONE NUMBER (Include Area Code) (202) 761-4741

This page is intentionally blank.