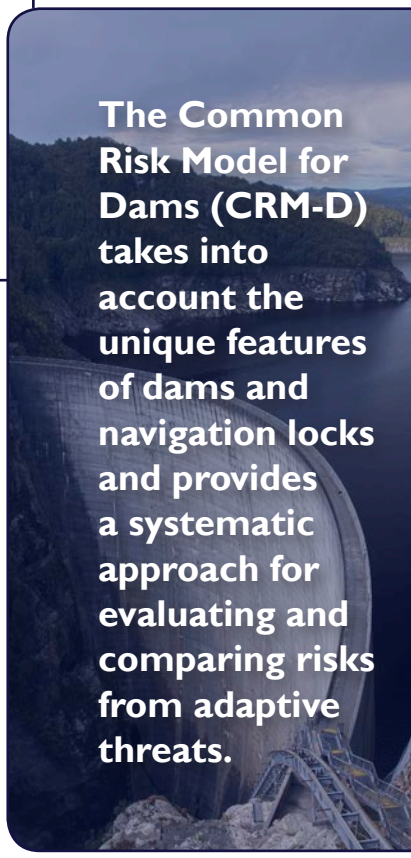
ASSESSING SECURITY RISKS USING THE COMMON RISK MODEL FOR DAMS

Yazmin Seda-Sanabria, Enrique E. Matheu, J. Darrell Morgeson, Yev Kirpichevsky, M. Anthony Fainberg, Jason A. Dechant, and Victor A. Utgoff

The Common Risk Model for Dams (CRM-D), developed as a result of collaboration between the U.S. Army Corps of Engineers (USACE) 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 similar infrastructures. The methodology provides a systematic approach for evaluating and comparing security risks across a large portfolio. Risk is calculated for attack scenarios (specific adversary using a specific attack vector against a specific target) by combining consequence, vulnerability, and threat estimates in a way that properly accounts for the relationships among these variables. The CRM-D can effectively quantify the benefits of implementing a particular risk mitigation strategy and, consequently, enable return-on-investment (ROI) analyses for multiple mitigation alternatives across a large portfolio.



In 2005, IDA initiated the development of the Common Risk Model (CRM) for evaluating and comparing risks associated with the nation's critical infrastructure. The model enables comparisons of calculated risks to assets and systems within and across critical infrastructure sectors.

A modified version of this model has been under development by IDA in collaboration with the U.S. Army Corps of Engineers (USACE) and the U.S. Department of Homeland Security (DHS). The modified model—the 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 adaptive threats across a large portfolio (Seda-Sanabria, Fainberg, and Matheu 2011a).

Risk is estimated for an attack scenario, which is defined as a specific adversary (e.g., a highly capable transnational terrorist group), a specific target (e.g., the main impoundment structure of a specific dam), and a specific attack vector (e.g., a cargo van loaded with explosives). Risk is defined as the expected value of loss and is a function of three variables: threat (T), vulnerability (V), and consequences (C):

$$R = f\,(\mathrm{T}, \mathrm{V}, \mathrm{C}). \qquad (1)$$

Threat is defined as the probability of an attack scenario attempted by the adversary, given the attack on one of the targets

in the portfolio under assessment, or P(A); vulnerability is defined as the probability of defeating the target's defenses, given that the attack is attempted, or P(S|A); and consequences are defined as the expected consequences of the attack, 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:

$$R=P(A)\times P(S|A)\times C.^{1} \qquad (2)$$

CRM-D also defines "conditional risk," or R_C, as risk for the attack scenario, given that this scenario is chosen:[2]

$$Rc=P(S|A)\times C. \qquad (3)$$

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

METHOD

The CRM-D methodology integrates the outputs of three separate models: consequences (external to CRM-D), vulnerability, and threat. Using modeling is a natural choice for estimating the outcomes of complex physical and economic processes, such as consequences from attack, but is equally important for estimating vulnerability and threat—variables that require more subjective input from subject matter experts (SMEs). Because there are many possible attack scenarios and because the set is continually changing, it is prohibitively costly and time consuming to elicit expert judgments on vulnerability and threat for every scenario and to repeat the elicitation process every time that a new scenario is introduced or old scenarios are modified. As a result, modeling is crucial when developing risk estimates in support of return-on-investment (ROI) analyses because the impacts on risk of potential risk-mitigation improvements need to be assessed quickly.

The vulnerability and threat models are based on data elicited from SMEs in a way that makes it possible to apply elicited SME judgment to any set of attack scenarios. The elicitations were conducted for estimating risk from highly capable, transnational adversary groups. Elicitations in support of estimating risk from other types of adversaries are currently under development. Because the adversaries' capabilities and/or intent are likely to change with time, elicitations should be repeated every few years or as deemed appropriate.

VULNERABILITY

To evaluate the vulnerability of a target to a specific attack by a specific adversary, a model of layered defenses is adopted. The defensive layers protecting a given target could potentially include

[1] The functional relationships among the variables are accounted for by estimating P(A) as a function of the other two variables, but there is no stochastic relationship because P(S|A) and expected consequences are estimated as point values, and not random variables. This justifies the use of the product function (Cox 2008).

[2] Note that the risk metric in Eq. (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.

national defenses (e.g., national counter-terrorism activities), local defenses (e.g., local law enforcement capabilities to detect and respond to potential attacks), and target defenses (e.g., onsite security systems and protective measures). The methodology for producing vulnerability estimates accounting for target defensive layers is described in detail in Seda-Sanabria et al. (2011b). The methodology for producing vulnerability estimates for national and local defensive layers is currently under development.

THREAT

Modeling threats 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 decision criteria change, their choice could 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.

CONSEQUENCES

As mentioned, consequence estimates are external inputs into CRM-D. They are typically measured in terms of loss of life and economic impact. To date, they have been generated by the USACE Modeling, Mapping, and Consequences (MMC) Production Center in conjunction with the U.S. Army Engineering Research and Development Center (ERDC).

RESULTS

In 2011, USACE initiated a pilot implementation of the CRM-D at a selected number of dams and navigation locks. Each project in this representative set had unique features, functions, and operational conditions that made it particularly suitable to test the capabilities of the methodology and its applicability to a large portfolio.

Risk was estimated in terms of expected loss of life and total economic damage for 16 attack scenarios associated with 9 dams and 2 attack vectors. Figure 1 shows the product of P(A) and P(S|A) plotted against economic consequences for attack scenarios (the targets are indexed by letters, and the attack vectors are indexed by numbers). Thus, risk in terms of economic consequences could be determined by multiplying the two coordinates together.

Figure 1 shows iso-curves that could represent thresholds of risk as determined by a decision maker (e.g., a portfolio owner). The curves trace those points for which risk is greater than $50 million (above the red line) and greater than $20 million (above the green line). Decision makers could hypothetically use such information to more readily identify those dams on which they choose to focus for developing investment alternatives. The risk values that would define these

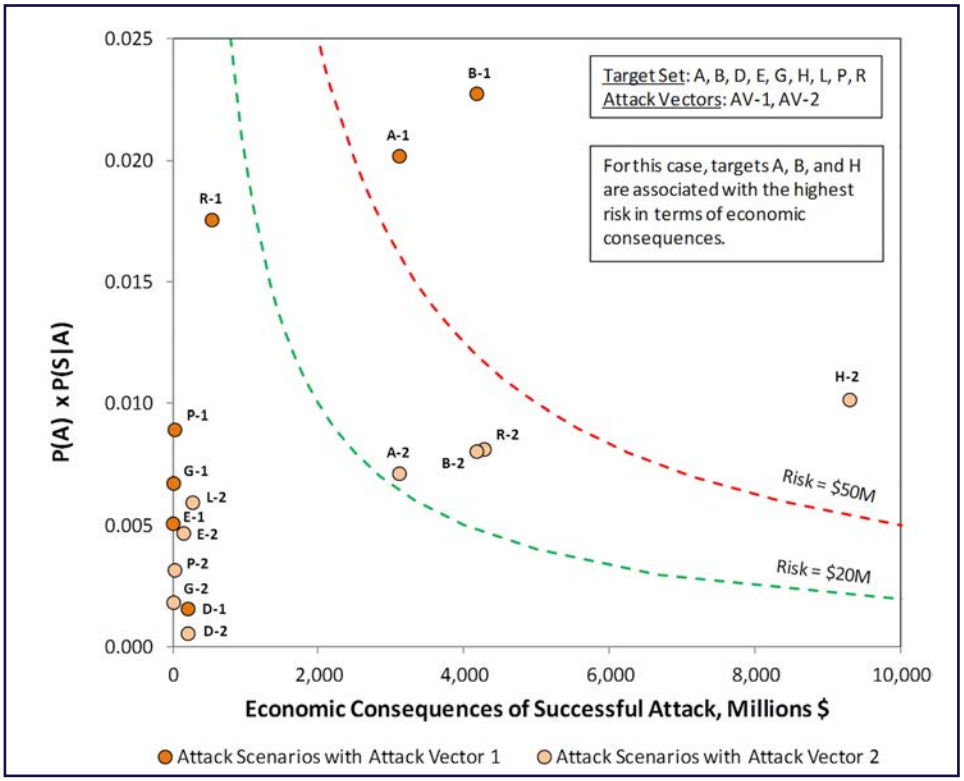


Figure 1. Scenarios by Economic Consequences of Success and Probability of Success.

curves could be chosen in accordance with decision-maker priorities.

A portfolio risk manager might wish to assess the impact of a particular investment on risk. For example, the addition of K12-rated vehicle barriers at seven of the projects where they had not been installed previously at a total cost of under $1 million could reduce portfolio risk given attack by about $66 million in expected economic damage and save an estimated 34 lives in an illustrative attack scenario. To decide whether adding K12-rated vehicle barriers is a worthy investment, a risk manager would have to assume or elicit from SMEs a predicted annual frequency of attacks in the portfolio and then use this information to compare this and other investments with the time-discounted values of the resulting risk reductions.

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 similar infrastructures.

Risk is calculated for attack scenarios as a function of consequences, vulnerability, and threat. The CRM-D 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 quantify the benefits of implementing a particular risk mitigation strategy and, consequently, enable ROI analyses for multiple risk mitigation alternatives across a large portfolio.

Ms. Seda-Sanabria is the National Program Manager of the Critical Infrastructure Protection and Resilience Program, Office of Homeland Security, U.S. Army Corps of Engineers.

Dr. Matheu is the Chief of the Critical Lifelines Branch in the Sector Outreach and Programs Division, Office of Infrastructure Protection, National Protection Programs Directorate, U.S. Department of Homeland Security.

Mr. Morgeson is a Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Master of Science in operations research from the Naval Postgraduate School.

Dr. Kirpichevsky is an Adjunct Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Doctor of Philosophy in government from Harvard University.

Dr. Fainberg is an Adjunct Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Doctor of Philosophy in particle physics from the University of California.

Dr. Dechant is a Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Doctor of Philosophy in public policy from George Mason University.

Dr. Utgoff is an Adjunct Research Staff Member in IDA's Strategy, Forces and Resources Division. He holds a Doctor of Philosophy in electrical engineering from Purdue University.

The full article was published in *Hydropower & Dams*, Issue Four, 2013

A Portfolio Approach to Security Risk Assessments

https://idacms.ida.org/upload/idanews/welch14/nsd4943.pdf

REFERENCES

Cox, Louis Anthony (Tony) Jr. 2008. "Some Limitations of 'Risk = Threat × Vulnerability × Consequence' for Risk Analysis of Terrorist Attacks." *Risk Analysis* 28 (6) (December): 1749–1761.

Seda-Sanabria, Yazmin, M. Anthony Fainberg, and Enrique E. Matheu. 2011a. "A Consistent Approach for Vulnerability Assessment of Dams," In *Proceedings of the 31st U.S. Society of Dams Annual Meeting and Conference*, 1117–1128. Denver, CO: U.S. Society on Dams.

Seda-Sanabria, Y., M. A., Fainberg, E. E. Matheu, J. D. Tressler, and M. L Bowen. 2011b. "Implementation of the Common Risk Model for Dams for Security Assessments of USACE Critical Infrastructure." Paper presented at the Dam Safety 2011 Conference, Washington, DC, September 25–29.