IDA | Research Insights

October 2018

# Assessing Cyber Security Risk for the Dams Sector

Jason A. Dechant (jdechant@ida.org), Reginald N. Meeson (rmeeson@ida.org), and James D. Morgeson (jmorgeso@ida.org)

Working with the U.S. Army Corps of Engineers and the Department of Homeland Security, IDA developed the Cyber Security Module (CSM) of the Common Risk Model for Dams to help integrate physical security and cyber security of the portfolio of dams that the U.S. Army Corps of Engineers maintains. The CSM develops a concise report of cyber risk at dams, which can then be used to determine whether dams—part of the nation's critical infrastructure—are adequately protected.

**The CSM determines a dam's cyber vulnerability rating (Matrix 1).** Cyber vulnerability is a semi-quantitative rating (from extremely low to extremely high) that reflects the level of protection provided by the architecture type of the industrial control system (ICS) at the dam in combination with one of six increasingly strong cyber defense packages (0 through 5). These packages provide a combination of physical defenses (gates, access controls, and surveillance systems), personnel measures (background checks and cyber security training), and cyber controls (computer access controls and system monitoring).

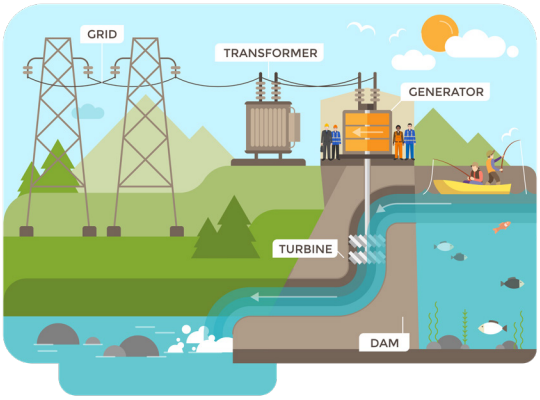
| Cyber defense package | ICS architecture type | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 0 | Extremely high | Extremely high | Extremely high | Extremely high |
| 1 | Very high | High | Moderate | Low |
| 2 | High | Moderate | Low | Extremely low |
| 3 | Moderate | Low | Very low | |
| 4 | Low | Very low | Extremely low | |
| 5 | Very low | | | |

Matrix 1. Cyber vulnerability rating

**The CSM combines cyber vulnerability rating with an estimate of the consequences of a successful cyberattack to estimate cyber risk (Matrix 2).** Consequences are measured in economic and human losses that can result from damage to a dam's critical functions (flood risk management, hydropower generation, navigation, or water supply) caused by cyberattack. Potential damage from a successful cyberattack is derived using a set of rule-based cyber scenarios applicable to specific dams given their critical functions. For example, if a dam's hydropower governors, which control flow of water through a turbine, are cyber vulnerable, damage from a cyberattack could include generator destruction and hydropower loss. A consequence level of 1 reflects the lowest estimated economic and human losses from such damage, and consequence level 5 reflects the highest. The CSM combines consequence level with cyber vulnerability rating to derive a cyber risk rating from very low to very high.

| Cyber vulnerability rating | Consequence level | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 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 |
| | Very low | Very low | Very low | Low | Low |

Matrix 2. Cyber risk rating




**The rigorous tools in the broader Common Risk Model for Dams suite estimate both physical and cyber security risks to U.S. dams.** These estimates can inform decisions about investment needed to mitigate those risks and reduce loss from both physical attacks and cyberattacks on dams.

Based on "Operationalizing Cyber Security Risk Assessments for the Dams Sector," K. Burns, J. Dechant, D. Morgeson, and R. Meeson, Jr., *IDA Research Notes*, Spring 2018: 34–41. See also IDA P-9295, *The Common Risk Model for Dams, Volume V: Cyber Security for Industrial Control Systems*, J. D. Morgeson, R. N. Meeson, W. R. Simpson, Jason A. Dechant, and A. C. Hermes, February 2017. Research was sponsored by the Director of Cost Assessment and Program Evaluation in the Office of the Secretary of Defense and by the U.S. Army Corps of Engineers.

NS D-9173


4850 Mark Center Drive
Alexandria, VA 22311-1882
ida.org