

Security Risk Assessment Methodologies (RAM)



Summary

In the mid 1970s, the Department of Energy (DOE) designated Sandia as the Lead Laboratory for development of physical security technology and funded Sandia to develop a technical capability in security modeling and systems analysis, security equipment and components, and security systems engineering, integration and implementation.

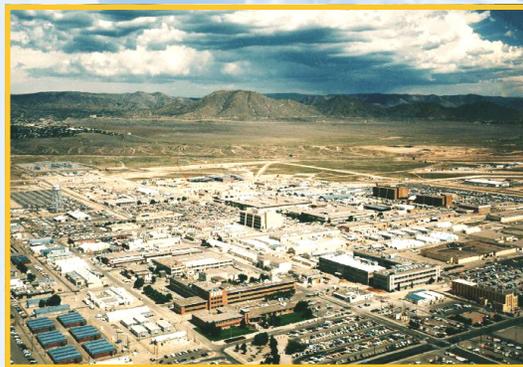
For more than 30 years, Sandia has applied performance-based methods for designing and evaluating physical protection systems (PPS). This approach has been applied for many years to high-consequence government facilities, and in the last several years this approach has been modified, tested, and applied to various critical



infrastructures such as federal dams, power utilities, water utilities, etc. While non-nuclear sites, facilities, and critical infrastructures may not require the highest levels of security used at nuclear weapons sites, the approach is the same. The foundations of a risk assessment methodology (RAM) is the evaluation and design of an integrated performance-based system.

Types of RAMs:

- **BioRAM** for Biological Facilities
- **RAM-C™** for Communities
- **RAM-CF™** for Chemical Facilities
- **RAM-CI** for Critical Infrastructures
- **RAM-DSM** for Dams
- **RAM-E** for Energy Infrastructures
- **RAM-PSM** for Prisons
- **RAM-TSM** for Transmissions
- **RAM-W™** for Water Utilities



Licensing & Partnering Status:

Various license and partnering options are available. Please contact the Intellectual Property department to discuss.

EACH RAM IS COMPRISED OF:

- Planning
- Threat assessment
- Site characterization
- Consequence assessment
- System effectiveness
- Risk analysis
- Risk management and reduction

MORE INFORMATION AVAILABLE AT:

- www.Sandia.gov/RAM

INTELLECTUAL PROPERTY & LICENSING CONTACT

Craig Smith
925.294.3358
casmith@sandia.gov