LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-470575

Assessing Vulnerabilities, Risks, and Consequences of Damage to Critical Infrastructure

N. Suski, C. Wuest

February 15, 2011

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Assessing the Vulnerabilities, Risks, and Consequences of Damage to Critical Infrastructure

Nancy Suski, Lawrence Livermore National Laboratory
Craig Wuest, Lawrence Livermore National Laboratory

Since the publication of *"Critical Foundations: Protecting America's Infrastructure,"* there has been a keen understanding of the complexity, interdependencies, and shared responsibility required to protect the nation's most critical assets that are essential to our way of life. The original 5 sectors defined in 1997 have grown to 18 Critical Infrastructures and Key Resources (CIKR), which are discussed in the 2009 *National Infrastructure Protection Plan (*NIPP*)* and its supporting sector-specific plans. The NIPP provides the structure for a national program dedicated to enhanced protection and resiliency of the nation's infrastructure.

Lawrence Livermore National Laboratory (LLNL) provides in-depth, multi-disciplinary assessments of threat, vulnerability, and consequence across all 18 sectors at scales ranging from specific facilities to infrastructures spanning multi-state regions, such as the Oil and Natural Gas (ONG) sector. Like many of the CIKR sectors, the ONG sector is comprised of production, processing, distribution, and storage of highly valuable and potentially dangerous commodities. Furthermore, there are significant interdependencies with other sectors, including transportation, communication, finance, and government. Understanding the potentially devastating consequences and collateral damage resulting from a terrorist attack or natural event is an important element of LLNL's infrastructure security programs.

Our work began in the energy sector in the late 1990s and quickly expanded other critical infrastructure sectors. We have performed over 600 physical assessments with a particular emphasis on those sectors that utilize, store, or ship potentially hazardous materials and for whom cyber security is important. The success of our approach is based on building awareness of vulnerabilities and risks and working directly with industry partners to collectively advance infrastructure protection. This approach consists of three phases:

The *Pre-Assessment Phase* brings together infrastructure owners and operators to identify critical assets and help the team create a structured information request. During this phase, we gain information about the critical assets from those who are most familiar with operations and interdependencies, making the time we spend on the ground conducting the assessment much more productive and enabling the team to make actionable recommendations.

The *Assessment Phase* analyzes 10 areas: Threat environment, cyber architecture, cyber penetration, physical security, physical penetration, operations security, policies and procedures, interdependencies, consequence analysis, and risk characterization. Each of these individual tasks uses direct and indirect data collection, site inspections, and structured and facilitated workshops to gather data.

Because of the importance of understanding the cyber threat, LLNL has built both fixed and mobile cyber penetration, wireless penetration and supporting tools that can be tailored to fit customer needs.

The *Post-Assessment Phase* brings vulnerability and risk assessments to the customer in a format that facilitates implementation of mitigation options. Often the assessment findings and recommendations are briefed and discussed with several levels of management and, if appropriate, across jurisdictional boundaries. The end result is enhanced awareness and informed protective measures. Over the last 15 years, we have continued to refine our methodology and capture lessons learned and best practices. The resulting risk and decision framework thus takes into consideration real-world constraints, including regulatory, operational, and economic realities.

In addition to "on the ground" assessments focused on mitigating vulnerabilities, we have integrated our computational and atmospheric dispersion capability with easy-to-use geo-referenced visualization tools to support emergency planning and response operations. LLNL is home to the National Atmospheric Release Advisory Center (NARAC) and the Interagency Modeling and Atmospheric Assessment Center (IMAAC). NARAC/IMAAC has capabilities to respond to toxic industrial chemical spills, nuclear-power plant accidents, fires, chemical/biological agents, radiological/nuclear devices (RDDs, INDs), and other airborne hazards.

Our web-based systems provide hazards assessments of critical infrastructure for defensive planning and can provide infrastructure operators and emergency responders with a baseline for planning and exercises. LLNL's infrastructure security web mapping services facilitate dissemination of technical information for all phases of disaster management. Examples of some of these products are shown in the Figure 1.

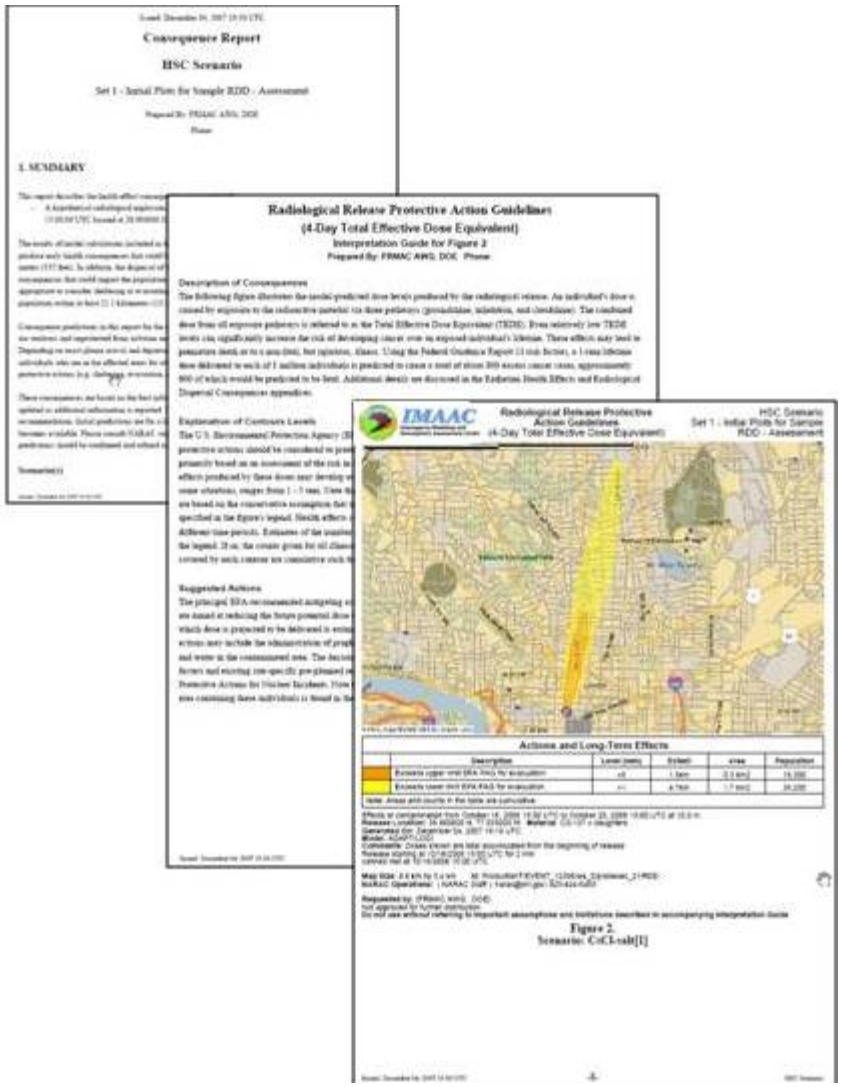

Figure 1. Consequence assessment products guide response decisions on evacuation, sheltering, relocation and worker protection

Examples of assessments performed under the auspices of the California National Guard, include several petroleum refineries, a strategic assessment of the California petroleum pipeline system, the West Coast Maritime System, and the California Electricity Grid. Strategic assessments typically involve a larger of region of critical infrastructure and are focused on interconnectivities and nodal analysis, rather than individual facilities. Other facility-specific assessments include detailed information on hazardous materials and the potential impacts of atmospheric releases on surrounding populations. These assessments can be integrated into larger maps (as shown in Figure 2) along with other critical infrastructure information to better

understand the system-wide impacts of an event and plan emergency response operations.

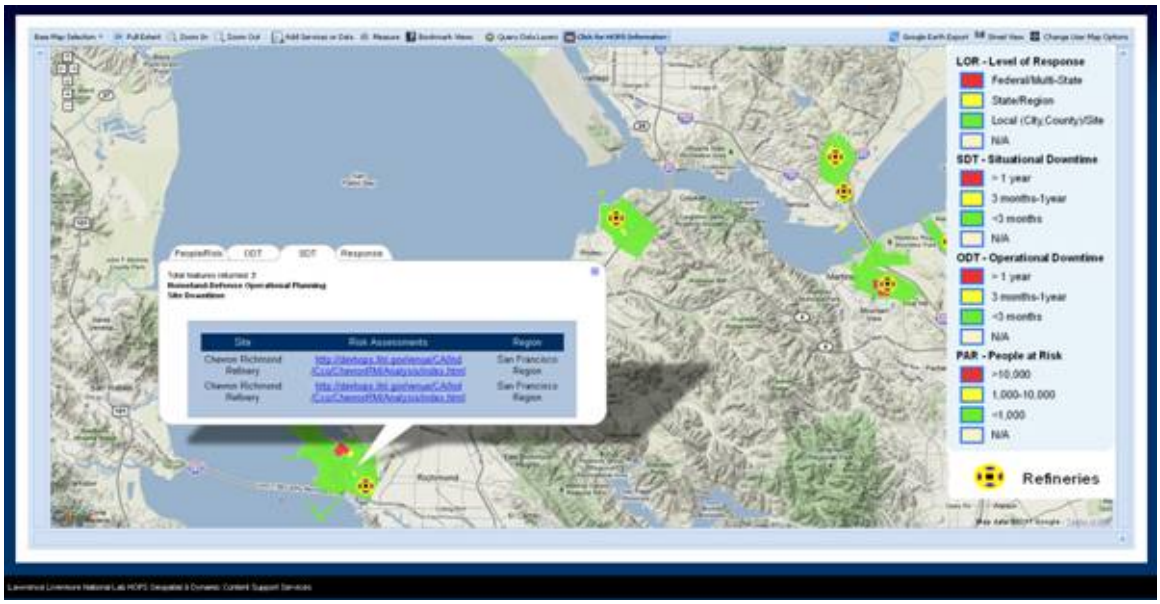

Figure 2. This map illustrates the locations of refineries in the San Francisco Bay area. The colors indicate potential site downtime, as noted in the legend. The Information Window provides descriptions of the site and a link to detailed analysis. The site can be investigated further by selecting additional tabs within the Information Window.

Our experience has shown that this kind of systems approach to infrastructure security and response planning provides a mechanism for federal, state and local governments to work with private infrastructure owners and operators to meet the over-arching goal of the National Infrastructure Protection Plan: "…to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency."

Contact information:

Nancy Suski
925-423-6046
suski2@llnl.gov

Craig Wuest
925-423-2909
wuest1@llnl.gov