



LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Vulnerability And Risk Assessment Using The Homeland-Defense Operational Planning System (HOPS)

R. L. Durling, Jr., D. E. Price, K. K. Spero

January 14, 2005

International Symposium on Systems and Human Science
San Francisco, CA, United States
March 9, 2005 through March 11, 2005

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

**VULNERABILITY AND RISK ASSESSMENT USING THE HOMELAND-DEFENSE
OPERATIONAL PLANNING SYSTEM (HOPS)**

Ronald L. Durling, Jr., David E. Price, Kimberlee K. Spero

Lawrence Livermore National Laboratory, 7000 East Avenue, L-182, Livermore California, 94550

VULNERABILITY AND RISK ASSESSMENT USING THE HOMELAND-DEFENSE OPERATIONAL PLANNING SYSTEM (HOPS)

ABSTRACT

For over ten years, the Counterproliferation Analysis and Planning System (CAPS) at Lawrence Livermore National Laboratory (LLNL) has been a planning tool used by U.S. combatant commands for mission support planning against foreign programs engaged in the manufacture of weapons of mass destruction (WMD). CAPS is endorsed by the Secretary of Defense as the preferred counterproliferation tool to be used by the nation's armed services.

A sister system, the Homeland-Defense Operational Planning System (HOPS), is a new operational planning tool leveraging CAPS expertise designed to support the defense of the U.S. homeland.

HOPS provides planners with a basis to make decisions to protect against acts of terrorism, focusing on the defense of facilities critical to U.S. infrastructure. Criticality of facilities, structures, and systems is evaluated on a composite matrix of specific projected casualty, economic, and sociopolitical impact bins. Based on these criteria, significant unidentified vulnerabilities are identified and secured. To provide insight into potential successes by malevolent actors, HOPS analysts strive to base their efforts mainly on unclassified open-source data. However, more cooperation is needed between HOPS analysts and facility representatives to provide an advantage to those whose task is to defend these facilities.

Evaluated facilities include: refineries, major ports, nuclear power plants and other nuclear licensees, dams, government installations, convention centers, sports stadiums, tourist venues, and public and freight transportation systems.

A generalized summary of analyses of U.S. infrastructure facilities will be presented.

BACKGROUND

The Counterproliferation Analysis and Planning System (CAPS) at Lawrence Livermore National Laboratory (LLNL) has been a planning tool used by U.S. combatant commands for mission support planning against foreign programs engaged in the manufacture of weapons of mass destruction (WMD) over the past twelve years. CAPS is endorsed by the Secretary of Defense as the preferred counterproliferation tool to be used by the nation's armed services. The CAPS Program provides a powerful database and engineering tools for assessing various processes (chemical, biological, nuclear, metallurgical, etc.) that proliferants use to build weapons of mass destruction and their delivery systems. By analyzing a country's specific approach to weapons production, we can pinpoint critical processing steps or production facilities which, if denied, would prevent that country from acquiring weapons of mass destruction, and we can pinpoint vulnerabilities which can then be exploited. The CAPS Program also assesses the consequences of a decision to interfere with suspected weapons development facilities.

There are four steps in creating the CAPS database. CAPS analysts: 1) model the set of chemical, biological, nuclear and missile manufacturing processes used to generate WMD and their delivery systems; 2) analyze a country's specific approach to WMD production from the possible sets; 3) pinpoint critical processing steps or production facilities which, if denied, would prevent that country from producing WMD; and 4) assess the health and environmental consequences of intervention actions.

If a consequence analysis is required, CAPS uses state-of-the-art software, climatology and terrain data to model the effects of the dispersal of toxic materials. Real-time data is a keystone of CAPS. For example, analysts can access a particular location and request a depiction of a plume release affected by winds blowing at that moment at the site.

CAPS consequence assessments provide military planners credible, documented estimates of collateral damage and include near real-time crisis action planning requests with little or no advanced notice. The system uses a secure communications network that transmits its critical data, analyses, and consequence assessments directly to military users worldwide. It comprises more than ten thousand web pages of information. During the early stages of Operation Iraqi Freedom, the number of hits increased to over one million per month.

STRUCTURE OF CAPS ANALYSES

CAPS analyses are categorized based on the degree of detail in the analysis

- A Level 1 analysis is a country-level identification of all sites that contribute to a specific WMD program
- A Level 2 (site-level) analysis identifies the layout and function of buildings on a particular site.
- A Level 3 (country program) analysis integrates the Level 1 and Level 2 analyses to identify the critical path for a country's WMD program by process, precursor, import, or technology.
- A Level 4 (building-level) analysis provides identification of the key components inside the most important building or buildings of an evaluated facility.
- A Level 5 (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability, or CARVER) analysis identifies the vulnerabilities of the key components identified in the Level 4 analysis.
- A Level 6 analysis identifies direct and indirect precision and network-centric effects on the processes analyzed in the Level 4 and 5 analyses.

CAPS has a potential for applications far beyond its original mission, especially in service to homeland security. This analysis and information system offers the possibility of assisting civil government in activities ranging from deliberate planning to disaster relief to emergency response. A sister system, the Homeland-Defense Operational Planning System (HOPS), is being used to support homeland defense activities in several states.

THE HOMELAND-DEFENSE OPERATIONAL PLANNING SYSTEM

The Homeland-Defense Operational Planning System (HOPS) is a new operational planning tool based on the CAPS structure and leverages CAPS expertise in exploiting vulnerabilities for protection of critical infrastructure to support the defense of the U.S. homeland. The close organizational connection between CAPS and HOPS permits managers in both programs to readily leverage CAPS analytic expertise as well as technologies and

analytic tools as they become available. The analyses that HOPS requires have their own specific attributes, and additional experts have been brought into the organization to meet these demands.

HOPS is sponsored by the California National Guard and has been vetted in several state and national level exercises. HOPS has also been recognized by multiple organizations as being superior to existing planning tools.

HOPS provides planners with the basis to make decisions to defend against acts of terrorism, focusing on the defense of facilities critical to the infrastructure of the United States and its territories. HOPS is currently involved in assisting multiple states as they establish their Protection of Critical Infrastructure plans. The program further provides strategic planners with a means to seamlessly communicate with other elements associated with defense and emergency response, and provides computer-based tools to support planning and response activities. HOPS has been an integral part of several exercises involving response to postulated WMD events in the United States.

STRUCTURE OF HOPS ANALYSES

There are four major aspects to the program:

- Criticality assessments of high value facilities. These assessments provide high-resolution analyses that identify the specific attributes of a facility that make it critical as well as its impact to the nation or state were it to be compromised.
- Vulnerability assessments of critical infrastructures associated with industry, agriculture, transportation, government/military installations, and large public structures such as sports arenas and convention centers. When appropriate, these assessments involve systematic analyses of the infrastructure to identify single points of failure and other critical nodes.
- A robust communications network that enables strategic planners engaged in homeland-defense to access the HOPS database to make decisions for strategic planning, and to communicate with subordinate and parallel organizations engaged in homeland-defense and to emergency responders in the event of an attack. HOPS is designed to reach its analysts directly at their work desks by operating on whatever classified or unclassified networks are required, including JWICS and SIPRNet (secure communications networks used by the Department of Defense).

- Analytic tools, such as three dimensional atmospheric plume modeling that utilizes real time wind conditions and conflict simulations that model the effectiveness of security plans. HOPS is also able to integrate with current data sets maintained by cities, counties or other jurisdictions. In this way organizations can leverage data that is already being maintained without requiring additional effort or resources.

HOPS analyses are generally equivalent to a Level 4 analysis in CAPS, but there are several distinct differences. Most significantly, while CAPS looks at the criticality of a site in terms of stopping or delaying the process for building WMD, criticality of sites within HOPS is evaluated on a composite matrix of specific projected casualty, economic, and sociopolitical impact bins. Another significant difference is that HOPS analysts strive to base their efforts initially on unclassified open-source data to provide insight into potential successes by malevolent actors.

CRITICALITY ANALYSIS METHODOLOGY

Criticality analysis attempts to prioritize infrastructure elements within a given area or sector of interest by the magnitude of the impacts created by the element's destruction or disablement. The ranking is performed based on "element criticality," defined as a function of the magnitude of potential casualties, economic impacts, and sociopolitical impacts.

In reality, the element's criticality is affected, to some degree, by the cause of damage – for example, the sociopolitical effects of a terrorist attack resulting in the destruction of an airport terminal will be very different from those same effects resulting from the collapse of the terminal due to poor structural design. However, one must also keep separate the magnitude of effect due to the specific attack mode compared to the effect posed by the element. Any attack has an effect. Criticality analysis attempts to identify those elements that by their very nature magnify the effect of attack. Examples include national monuments and facilities storing large quantities of hazardous materials.

Vulnerability is a function of accessibility, attack deterrence capability (security measures, protective force), and the element's "hardness" or physical ability to withstand the attack or contingency stress. In a HOPS analysis, the criticality of an element is not influenced by its vulnerability. For example, a sports arena is always critical as a high value terrorist target

because of the potentially high casualty rate regardless of the security and protective measures deployed.

It is assumed that a terrorist organization will consider the vulnerability of a target in a way that matches their available resources and capabilities with feasible interdiction or defeat modes. This would be done separately from assessing the criticality or value of the target that is, in turn, dependent only on the extent of potential casualties, economic impacts, and sociopolitical impacts, as discussed below.

Facilities deemed to be highly critical yet invulnerable, as well as facilities not critical but highly vulnerable, may not be of significant concern to homeland defenders. In both cases the interest may not be relevant, but it is the broad mix between these two extremes upon which HOPS focuses its efforts.

Casualties

Typically, the extent of casualties is thought of as “body count” resulting from explosion, fire, flood, structural collapse, or exposure to toxic chemical, radiation, chemical warfare agent, or biological agent.

A separate consideration is to distinguish between the casualties related to the type of a terrorist assault device used and the casualties that are related to the inherent characteristics of the infrastructure element. In a HOPS analysis, the focus is primarily on the effects stemming from the inherent characteristics of the infrastructure element being analyzed and not on the effects of different types of assault devices or modes of interdiction.

Key considerations in assessing the potential extent of casualties are:

- Type and quantity of hazardous materials stored or processed onsite, or those used in the attack
- Presence of materials that, upon purposeful contamination and subsequent consumption, can result in significant health impacts to offsite population – for example, a food processing plant could be of high value as a target for a surreptitious terrorist attack involving poisoning of the food or its ingredients.
- Number of people or workers present in the immediate impact area
- Proximity to population centers downwind of the impact area
- Population density of the affected downwind areas

Some cases may require additional modeling of thermal effects, blast overpressure effects, or atmospheric dispersion. A wealth of information that is needed for casualty assessment is available in open source literature and the public domain.

Economic Impacts

In the HOPS analyses, a distinction is made between the direct and indirect economic consequences of an attack.

Key considerations in assessing direct economic impacts are as follows:

- Damage repair/restoration cost
- Lost revenue and profit due to disruption of element's operations
- Value of lost inventory or intrinsic value of damaged goods

Key considerations in assessing indirect economic impacts are:

- Duration of damage restoration effort
- Upstream and downstream ripple effects
- Effects of changes in customer spending patterns
- Loss of jobs
- Healthcare costs
- Government expenditures (emergency services, security, protection, etc.)
- Loss of efficiencies in patterns (road detours, makeshift offices etc.)

Indirect impacts also include changes in purchasing or spending patterns resulting from public fear – for example, both airline and tourism industries were severely impacted worldwide by the events of 9/11. In the nuclear power industry, direct costs associated with damage or destruction of a nuclear power plant will include the cost of replacement part procurement, installation and reconstruction. Indirect costs primarily include the cost of replacement power, which could be on the order of a million dollars per day.

While direct costs can be estimated with fair accuracy for most cases using standard techniques, the indirect costs are generally more difficult to estimate owing to the complexities involved and current unavailability of reliable models.

Sociopolitical Impacts

One of the main objectives of a terrorist organization is to instill widespread fear, anxiety, or outrage leading to instabilities and disruptions in the normal functioning of a society. Such instabilities and disruptions may take the form of reduced productivity, introduction of freedom-curtailing security measures, pressure on government to conform to the terrorists demands, and attendant changes in the laws, political climate, foreign policy, and even military actions abroad.

Assessing sociopolitical impact is the most difficult aspect of criticality because of the complexity and uncertainties involved in determination of specific potential consequences (especially long-term consequences), lack of clear metrics, and inherent reliance on subjective judgment of the analyst(s) in dealing with many intangible factors. In assessing sociopolitical consequences, the analyst must also consider loss of life and economic effects, past societal responses, political climate, and symbolic value of a target to the society and to terrorists.

Criticality Assessment Methodology

The criticality assessment methodology encompasses the following steps:

- 1) Gather and review relevant information about the competing infrastructure elements within a given venue.
- 2) Eliminate those elements that are clearly of negligible criticality (i.e., those elements where the potential casualty rate, economic impacts, and sociopolitical impacts would be insignificant).
- 3) Systematically assess the remaining elements using both qualitative and, if at all possible, quantitative arguments.
- 4) Conduct a critical review of the draft assessment by qualified peer reviewers.

Each element is assessed and rated with regard to each category (casualties, economic impacts, and sociopolitical impacts) in terms of high, moderate, low, or minor impact. The following table provides example criteria for these categories:

METRIC	HIGH	MODERATE	LOW	MINOR
Casualty	≥ 5000 deaths	200 – 5000 deaths	1 - 200 deaths	No deaths
Economic	≥ \$1 billion	\$100 m - \$ 1 billion	\$10 m - \$100 m	≤ \$10 million

METRIC	HIGH	MODERATE	LOW	MINOR
Sociopolitical	Detriment to national security, government, or military readiness or functionality; Large multi-region/country impact; Unique, world-wide recognition, #1-3 in nation or world; Nationwide fear	Threat to national security, government, military; Multi-state impact; 3m – 10m people directly affected Regional landmark or government building, Top 10 in nation; Terrorism directed at national interest; Regional fear	Multi-city impact; 3m - 100,000 people directly affected Not unique, Not widely known; Widely known but not highly reported in media. Terrorism but locally directed; Limited fear	Local impact; ≤ 100,000 people directly affected Not unique, Not widely known; Low media coverage

A short narrative documents each assessment and provides the rationale and supporting discussion for the ratings assigned. The overall criticality of the element is then based on the individual criteria ratings and is generally the same as the highest individual criteria rating.

Field of Inquiry

The field of inquiry defines how the three factors that influence criticality (i.e., casualties, economic impacts, and sociopolitical impacts) are applied. At the venue or regional level, the task is to rate each individual facility in terms of its criticality relative to the other facilities within the venue or region of interest. Hence, it becomes important to consider and compare facility-specific indirect economic impacts and sociopolitical impacts.

Facilities that are assessed as highly critical are then subjected to analysis at the facility level to identify those specific systems, equipment, or elements that, upon failure, would disable the functioning of the entire facility over a long time, cause the release of hazardous materials, cause fire or explosion, or instill widespread public fear. The focus of a facility-level analysis is to identify the critical equipment or systems within the facility that result in greatest impact or effect.

ANALYSES

The facilities considered in HOPS are grouped into five major categories:

- Agriculture
- Industry

- Military/Government
- Sports/Civic
- Transportation

These categories were derived from Department of Homeland Security Sectors and Department of Commerce listings. They were consolidated and grouped into the five sectors based on input from the State level Critical Infrastructure lists.

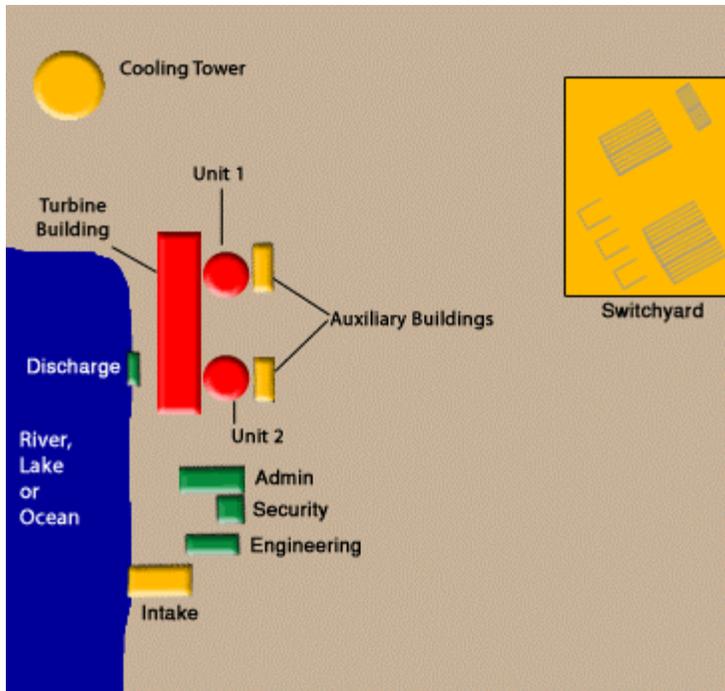
EXAMPLE ANALYSIS SUMMARIES

Facilities evaluated to date include refineries, major ports, nuclear plants and other nuclear material users, convention centers, sports stadiums, dams, transportation facilities, government installations, and public transportation.

Typically, risk and reliability analyses of nuclear power plants have focused on prevention of damage to the reactor core and resultant releases of radioactive material, and vulnerability analyses focus on physical security measures, i.e., “gates and guards”. However, this approach fails to recognize the high symbolic value resulting from an attack on a nuclear power plant, regardless of actual damage caused by the attack. Furthermore, any disruption of plant operation would result in a significant economic impact due to factors such as repair costs, replacement power costs, etc.

As introduced above, our analyses of domestic nuclear power plants were based solely on open source data found on the internet and other publicly available resources. This material included basic descriptions of the facilities, documents from public hearings regarding environmental and regulatory issues, up to a complete set of operator system training guides. A generic analysis summary is presented below to illustrate the HOPS structure and methodology.

The analysis presentation starts with an overview of the facility listing major components, as well as a satellite image and color-coded schematic that summarizes the criticality analysis for the facility, with red signifying the most critical. If there are important subsystems or structures in the facility, the schematic also allows the user to navigate to the desired analysis.



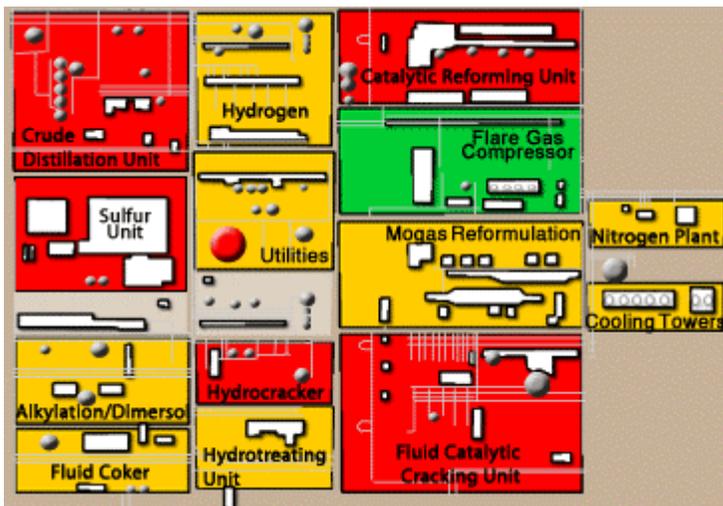
In the case of the generic nuclear facility depicted above, the two reactor containment buildings are deemed highly critical structures. Most would expect this to be the case from a casualty standpoint. However, although irradiated fuel is extremely hazardous, the robustness of the reactor vessel and the containment buildings themselves leads to a moderate criticality rating from a casualty standpoint. Rather, it is the economic impact that leads to high criticality. If the containment structures and major systems within them were damaged, the replacement time is judged to be significantly longer than other structures and systems at the plant, and the resultant costs for replacement power – on the order of a million dollars a day – would be significant. The turbine building is also highly critical, primarily due to economic concerns.

Once the most important structures have been identified, protective actions and other mitigation measures may be put in place. In some cases, structures and systems that were not previously identified as important may need additional security and mitigation measures.

In addition to nuclear power plants, HOPS has provided analyses of convention centers. Again the analysis presentation starts with an overview of the system showing floor plans and major components of the facility, such as utilities, air intakes and emergency generators. In the case of a convention center, criticality is a function of the event it is hosting, thereby leading the analysis to look at potential attacks on the population. An understanding of the facility's systems

and how they affect each room of the center is provided. In this way defenders can understand what they need to protect and responders have a path to follow should an event occur.

Criticality of refineries is similar to that of nuclear plants, in that economic criticality contributes significantly to overall criticality. However, due to the presence of large quantities of hazardous materials, such as anhydrous ammonia or amines (monoethanol amine, diethanol amine, and methyl diethanol amine) used for sulfur extraction and recovery, health consequences also contribute significantly to overall facility criticality. In the example refinery below, the crude distillation unit, fluid catalytic cracking unit, catalytic reforming unit, and hydrocracker are assigned a high criticality rating based on economic considerations. Additionally, failure of the anhydrous ammonia tank and the sulfur unit would each result in significant casualties due to the toxic release, thus they are also considered highly critical. Of the remaining areas, the hydrotreating unit is a moderately critical area due to potential consequences of a release of hydrogen sulfide from the unit. The remaining moderate criticality areas are identified based on economic impacts.



Our analyses have in many instances identified vulnerabilities not previously identified. Unfortunately, although the specifics are based on unclassified data, the results are sensitive, thus we cannot discuss them in any detail in any public forum.

CONCLUSIONS AND RECOMMENDATIONS

Many of the facilities we have evaluated, whether they be nuclear power plants, refineries, or seaports, are generally unwilling to share their information, even with a nationally recognized institution such as a National Laboratory. In many cases, there are concerns about releasing

proprietary information, but there is also the concern of inadvertent public dissemination for fear of incurring potential legal liability.

However, as we have repeatedly demonstrated, terrorists have access to the same information, and could conceivably reach the same conclusions with regard to heretofore unidentified vulnerabilities.

In addition, most facilities focus on physical security, while their true vulnerability may lie in the process or technology of their facility. While facilities are unwilling to unveil their physical security plans, they are often completely willing to talk about their processes. Thus, we strongly encourage more cooperation between HOPS analysts and facility representatives, either through sharing of additional information that may not be generally available to the public or by participating in the review process of HOPS analyses, such that we can provide a measurable advantage to those whose task is to defend these facilities.

We also encourage the facilities as they complete their risk and vulnerability assessments to focus on the technology and engineering aspects of their area, not simply the perimeter defense.