



Center for Risk and Security
The George Perkins Marsh Institute

CRS DISCUSSION PAPER 2005-02

Designing Infrastructure
for New Goals and Constraints*

Gordon R. Thompson
Research Professor

June 2005

CRS DISCUSSION PAPER 2005-02
Center for Risk and Security
The George Perkins Marsh Institute
Clark University
Worcester, MA

* This discussion paper was previously presented by the author during a U.S. Department of Homeland Security sponsored conference, "Working Together: R&D Partnerships in Homeland Security," Boston, Massachusetts, April 27-28, 2005.

DOCUMENT REPRODUCTION

This document is a discussion paper of the Center for Risk and Security (CRS), The George Perkins Marsh Institute, Clark University. CRS Discussion Papers are works in progress and views expressed in this paper are those of the author. CRS allows reproduction of this paper for personal and educational purposes. Any other reproduction of this paper is not permitted without written permission from CRS or its author.

CONTACT INFORMATION

Primary:

Gordon R. Thompson
Center for Risk and Security
The George Perkins Marsh Institute
Clark University
Phone: (617) 491-5177
Fax: (617) 491-6904
Email: gothompson@clarku.edu

Center:

Center for Risk and Security
The George Perkins Marsh Institute
Clark University
950 Main Street
Worcester, MA 01610
Phone: (508) 751-4622
Fax: (508) 751-4600
Email: crs@clarku.edu

SUGGESTED CITATION

Thompson, Gordon R., *Designing Infrastructure for New Goals and Constraints*, CRS Discussion Paper 2005-02, Center for Risk and Security, The George Perkins Marsh Institute, Clark University, June 2005.

ABOUT THE AUTHOR

Gordon R. Thompson, D. Phil., is a research professor at the George Perkins Marsh Institute and the executive director of the Institute for Resource and Security Studies, Cambridge, Massachusetts, an independent organization that he founded in 1984. He was educated in Australia and the UK, in engineering and science, obtaining his doctorate from Oxford University in 1973. Over the past three decades he has acquired wide experience with natural resource and international security issues. One of his major interests has been the environmental and security impacts of nuclear technologies. Dr. Thompson has coordinated multidisciplinary teams, organized international conferences and provided expert testimony in a variety of contexts.

ABSTRACT

Security has emerged as a major factor to be considered in designing national infrastructure. Sustainability – a concept typically interpreted as having environmental, social and economic dimensions – is a currently neglected factor that is at least equally important. These and other factors oblige contemporary designers of infrastructure networks and components to consider more goals and constraints than was previously thought to be necessary. This paper identifies design principles whereby security and sustainability concerns can be considered in the design process. Security design principles include: redundancy, independence and looser coupling of system elements; passive safety; fault tolerance; etc. Sustainability design principles include: dematerialization; industrial ecology; renewable supply of energy and materials; etc. Examination of one infrastructure design option – distributed generation of electricity – suggests that this option could potentially conform to both sets of principles. Similarities in the principles suggest that other design options could achieve the same outcome. These suggested findings deserve further investigation.

INTRODUCTION

This discussion paper was previously presented by the author during a U.S. Department of Homeland Security sponsored conference, “Working Together: R&D Partnerships in Homeland Security,” Boston, Massachusetts, April 27-28, 2005, at the conference poster session titled “Critical Infrastructure Protection.” That session addressed the potential for attacks on critical infrastructure – defined below – and the opportunities to counter such attacks. These matters fall under the general rubric, “homeland security.”

Security, although important, is not the only factor to be considered in designing a country's infrastructure. Indeed, other factors have dominated the design of much of the infrastructure that is currently in use in the USA. Over the coming years and decades, however, security is likely to receive a higher priority. During the same period, at least an equivalent priority should be assigned to another design factor that is currently neglected – sustainability. It is therefore important to know if security and sustainability are complementary or conflicting design factors.

This paper addresses the needs and opportunities to design infrastructure for new goals and within new, or newly recognized, constraints. Special attention is given here to security and sustainability. There is limited experience in designing for both factors. An infrastructure option that is briefly discussed here – distributed generation of electricity – could potentially provide improvements in both security and sustainability. That finding suggests that thorough investigation of a variety of design options would be fruitful.

INFRASTRUCTURE DESIGN CHALLENGES OF THE 21st CENTURY

Networks of infrastructure – both physical and virtual – are essential to the operation of a modern society. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets describes US critical infrastructure as follows [8]:

"The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. They consist of human capital and physical and cyber systems that work together in processes that are highly interdependent. They each encompass a series of key nodes that are, in turn, essential to the operation of the critical infrastructures in which they function. To complicate matters further, our most critical infrastructures typically interconnect and, therefore, depend on the continued availability and operation of other dynamic systems and functions."

Since the attacks of September 2001, it has become widely accepted that US infrastructure networks and their components need improved capabilities to resist attack. Such capabilities could limit damage if attacks occur in the future. Also, improved attack resistance could potentially reduce the incentive to attack. If critical targets are robust, attackers are less able to create damage of strategic significance.

During recent decades there has been growing recognition that human activity is placing a burden on the Earth's natural resources that is not sustainable, even as many people's basic needs remain unmet [9]. A recent global assessment of ecosystems has confirmed that many of these systems are in a state of accelerating degradation [5]. Environmental sustainability has become a practical imperative, and should be a major consideration in the design of infrastructure networks and their components. Human needs are also important. Thus, the vision we should aim for is a society that is sustainable in three respects: (i) environmentally; (ii) socially; and (iii) economically.

Another indication of pressure on resources is the growing acknowledgment that world oil production may reach a peak comparatively soon, perhaps during the present decade [3]. This phenomenon, and the need to limit emissions of greenhouse gases, will have significant implications for the design of infrastructure in the energy and transportation sectors and elsewhere.

The factors outlined above will require substantial changes in the deployed stock of infrastructure over the coming decades. Yet, many infrastructure components have lifetimes measured in decades, or in centuries in some instances. Accordingly, designers and decision makers involved in the development of new infrastructure components should take a long-range view, anticipating future needs.

CRITICAL INFRASTRUCTURE IN THE USA: MAJOR SECTORS AND SOME COMPONENTS

The US government groups the nation's critical infrastructure into eleven major sectors. Those sectors, with some illustrative data on the infrastructure components in each sector, are as follows [8]:

- Agriculture and Food: 1,912,000 farms; 87,000 food-processing plants
- Water: 1,800 federal reservoirs; 1,600 municipal wastewater facilities
- Public Health: 5,800 registered hospitals
- Emergency Services: 87,000 US localities
- Defense Industrial Base: 250,000 firms in 215 distinct industries
- Telecommunications: 2 billion miles of cable
- Energy: *Electricity*: 2,800 power plants *Oil and Natural Gas*: 300,000 producing sites
- Transportation: *Aviation*: 5,000 public airports *Passenger Rail and Railroads*: 120,000 miles of major railroads *Highways, Trucking, and Busing*: 590,000 highway bridges *Pipelines*: 2 million miles of pipelines *Maritime*: 300 coastal and inland ports *Mass Transit*: 500 major urban public transit operators
- Banking and Finance: 26,600 FDIC-insured institutions
- Chemical Industry and Hazardous Materials: 66,000 chemical plants
- Postal and Shipping: 137 million delivery sites

DESIGNING FOR MULTIPLE GOALS AND CONSTRAINTS

An infrastructure network is designed to meet a set of functional goals. For example, in the water sector, a supply network is designed to deliver a specified amount of potable water to a designated set of customers. The designer pursues that goal within various constraints. In the case of a water-supply network, geographic factors such as rainfall and topography have been, and will continue to be, major constraints. Across the spectrum of infrastructure, additional constraints are now coming into effect to address concerns about security and sustainability. New goals also come into effect as the economy evolves and people's expectations change. A designer today must, therefore, account for more goals and constraints than was previously thought to be necessary.

In a modern, industrialized society such as the USA, there is a rich array of current and anticipated technology. This asset allows a designer of infrastructure to meet a given functional goal through a variety of design options. Some options will, however, be more effective in satisfying the applicable constraints. As new goals and constraints come into effect, optimization points will change and new design options will become appropriate. Ideally, designers will be able to accommodate concerns about security and sustainability within the same option. Sometimes, however, security and sustainability will be conflicting design factors. In those instances, tradeoffs will be necessary.

When security issues become prominent, managers and decision makers tend to become more secretive, and government tends to limit citizen freedoms. While understandable, these tendencies undermine the open democracy that is fundamental to our prosperity and quality of life. Designers of infrastructure networks and components can contribute to resolving this dilemma. They can develop designs that are inherently robust, and that do not need to be protected by secrecy or the restriction of civil liberties.

DESIGN PRINCIPLES FOR SECURITY

Various principles are used in designing systems to be more resistant to attack. At present, there is no consensus on the definition and specification of these principles. A list of principles is offered here, as a starting point for further analysis, as follows:

- Dispersal
Spatial separation of potential targets can limit the damage from an attack.

- Hardening
Increasing the robustness of potential targets can prevent attack or limit the damage from an attack.

- Redundancy and independence of system elements
Designing the elements of a system to be redundant (not all of the elements are necessary) and independent (elements are not all vulnerable to the same influences) can increase the robustness of the system.

- Looser coupling of system elements
Decreasing the spatial, temporal and functional reliance of a system element on other elements (e.g., by adding buffer storage to a flow system) can increase the robustness of the system.

- Limiting hazardous inventories
Designing a process so that inventories of hazardous material are limited (e.g., by producing a toxic chemical on a just-in-time basis) can limit environmental and health impacts in the event of an attack.

- Fault tolerance and self-repair
Systems can be designed to automatically detect, survive and recover from faults of accidental or malicious origin.

- Passive safety
Systems and their elements can be designed so that natural forces (e.g., gravity, thermal radiation) move them to a safe state under fault conditions.

- Monitoring and response

Extensive monitoring can trigger pre-planned or pre-engineered damage-limiting responses such as: (i) intercepting attackers; (ii) conducting onsite damage control (e.g., fire suppression); or (iii) conducting onsite or offsite emergency response (e.g., evacuation).

Efforts have been made to employ security design principles, of the type discussed above, in the context of critical infrastructure. For example, designers of chemical-processing plants have developed the concept of inherent safety, and have pointed out that this concept can improve resistance to attack. To date, the concept of inherent safety has been applied to a limited extent, in part because the USA has a large inventory of installed chemical-processing plants and there is little new construction of such plants [4].

DESIGN PRINCIPLES FOR SUSTAINABILITY

A variety of principles have been articulated for design for sustainability. Despite the general neglect of sustainability, numerous instances can be identified in which principles of this type have been applied during recent decades [7]. The principles include:

- Decarbonization

Societal functions can be performed with reduced net emissions to the atmosphere of carbon dioxide and other greenhouse gases.

- Dematerialization

Environmental impacts from the performing of societal functions can be reduced by [6]:

- + Increasing the efficiency of material use – using less material to perform a given function;
- + Substituting lower-impact (e.g., lighter) materials for higher-impact materials;
- + Reusing or recycling materials; and
- + Reducing demand for new products (e.g., by greater emphasis on repair and upgrading, or by increasing the intensity of a product's use).

- Industrial ecology

Waste flows and environmental impacts from industrial and commercial operations can be reduced by [2]:

- + Simulating natural ecosystems in which waste from one process is an input to another process;
- + Limiting the scale and location of processes involving hazardous (e.g., toxic) materials; and
- + Limiting effluents to amounts within the absorptive capacity of the environment.

- Renewable energy and materials

Energy (e.g., wind power) and materials (e.g., wood) can be obtained from solar-driven processes.

- Efficient generation and use of energy

Generation of energy flows (e.g., electricity) from primary sources can become more efficient, and energy can be used more efficiently to provide services (e.g., lighting).

- Integrated assessment

The sustainability of an activity can be determined by assessing its environmental, social and economic impacts throughout its life cycle.

- Integrated design, planning and investment

Sustainable outcomes can be ensured by integrating a full spectrum of considerations (e.g., the need to account for ecosystem services) into design, planning and investment decisions related to infrastructure networks and their components.

- A service economy rather than a flow economy

Selling services (e.g., transport) rather than products (e.g., cars) can often allow functions to be performed in a more sustainable manner.

AN INFRASTRUCTURE DESIGN EXAMPLE; DISTRIBUTED GENERATION OF ELECTRICITY

At present, most electricity used in the USA is generated at large power plants. About six percent of total US generation, however, is by distributed-generation (DG) units [1]. These units have capacities as small as a few kWe and are at diverse locations. They often generate heat and electricity, and export electricity that is not needed onsite.

Improvements in technology could substantially increase the role of distributed generation. For example, if photovoltaic cells become significantly cheaper, then they will be cost-competitive electricity sources and could be widely installed on rooftops. R&D on photovoltaic cells is proceeding with the aim of realizing this vision. Other technologies with distributed-generation application are also the subject of R&D. For example, the US Department of Energy has a program to develop solid-oxide fuel cells (FCs). The program seeks to develop cost-competitive fuel cells and FC-turbine hybrids that can be fueled with synthesis gas from coal or biomass, achieve efficiencies as high as 60-70 percent, and discharge an effluent consisting only of water and carbon dioxide [1]. The carbon dioxide could, in principle, be piped to a location where it is sequestered by underground injection.

If the needed technology developments occur, and the role of distributed generation grows substantially, then three types of security benefit could arise. First, the roles of central generation and long-distance transmission of electricity would be reduced, thereby increasing the

robustness of US electricity networks. Second, distributed generation could displace nuclear-generated electricity and the associated risks. Third, DG units could use renewable forms of energy (sun, wind, biomass) or coal, thereby displacing imported liquefied natural gas and its associated risks.

At the same time, expanded use of distributed generation could potentially yield three types of sustainability benefit. First, DG units fueled by coal or biomass, and with sequestration of carbon dioxide, could yield clean power that is greenhouse-neutral when fueled by coal and greenhouse-reducing when fueled by biomass. Second, DG units powered by sun or wind could yield clean, greenhouse-neutral power with low environmental impacts. Third, distributed generation could promote community development and local employment.

CONCLUSIONS

The preceding discussion shows that distributed generation of electricity is an infrastructure design option that could potentially meet both security and sustainability constraints. Examination of the design principles for security and sustainability suggests that distributed generation is not a unique example. There are areas of similarity in these principles, suggesting that many other infrastructure design options could achieve the same outcome. A much deeper investigation is required to determine if these suggested findings are accurate. More generally, considerable research and practical experience will be needed to determine the full potential for designing infrastructure to meet the goals and constraints of the 21st century.

REFERENCES

- [1] Department of Energy, *Distributed Generation: Ensuring Energy Security, Reliability and Efficiency* (Morgantown, West Virginia: National Energy Technology Laboratory, US Department of Energy, June 2003).
- [2] Garner, Andy, and Gregory A. Keoleian, *Industrial Ecology: An Introduction* (Ann Arbor, Michigan: National Pollution Prevention Center for Higher Education, University of Michigan, November 1995).
- [3] Hirsch, Robert L., Roger H. Bezdek and Robert M. Wendling, "Peaking Oil Production: Sooner Rather Than Later?" *Issues in Science and Technology*, Volume XXI, Number 3, Spring 2005, pp 25-30.
- [4] Mannan, Sam, *Challenges in Implementing Inherent Safety Principles in New and Existing Chemical Processes* (College Station, Texas: Mary Kay O'Connor Process Safety Center, Chemical Engineering Department, Texas A&M University System, August 2002).
- [5] Stokstad, Erik, "Taking the Pulse of Earth's Life-Support Systems", *Science*, Volume 308, 1 April 2005, pp 41-43. (News story about the Millennium Ecosystem Assessment.)
- [6] van der Voet, Ester, Laurant van Oers and Igor Nikolic, "Dematerialization: Not Just a Matter of Weight", *Journal of Industrial Ecology*, Volume 8, Number 4, 2005, pp 121-137.
- [7] von Weizsacker, Ernst, Amory B. Lovins and L. Hunter Lovins, *Factor Four: Doubling Wealth, Halving Resource Use* (London: Earthscan Publications, 1998).
- [8] White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: The White House, February 2003).
- [9] World Commission on Environment and Development, *Our Common Future* (Oxford: Oxford University Press, 1987).