A Brief Note on Resilience in Engineering

Laura J. Steinberg
Syracuse University
INSCT Workshop
January 16, 2009

Resilience in engineering is typically associated with the ability of a technology/physical asset(s) to continue to provide the services it was designed for, in the wake of changes or attempted changes to its "normal" operating environment. For example, a water supply system which is resilient to a contamination attack might employ all or some of the measures below:

- Guns , gates and guards measures:
  - Restricted/guarded assess to water supply reservoirs, water tanks, treatment works etc.
  - System for identifying authorized entries into facilities
  - Intruder detections systems
  - Response plan with law enforcement/DOD
- Design Criteria:
  - Use of design and construction requirements for physical infrastructure based on forces to be encountered during an extreme event e.g. blast-proofing
  - Redundancy
    - Duplication of facilities e.g. 2 elevated water tanks
    - System redundancy e.g. linkage to other jurisdictions' water supply; design of piping network for multiple water delivery paths
  - Operational measures:
    - Change to non-hazardous compounds e.g. replace chlorine gas with ultraviolet disinfection
    - "culture of safety"
    - Response plan and training
- Monitoring measures
  - In-line sensors for detection of changes in water characteristics, or changes in pressure
  - Laboratory testing for anomalous compounds
  - Procedures to evaluate and investigate notification from staff or water consumers of suspicious water quality
- Warning systems
  - Methods to communicate with the public and other entities that the water quality may have been compromised
- Security of computer systems – SCADA
- Business continuity measures

In this list, it is notable that some measures might best be classed as mitigation measures to prevent the success of an attack, while others are response measures to an attack which is intended or has occurred. Also, most of the measures, with the notable exception of guns, gates, and guards, provide resiliency against natural disasters and technological disasters also, reinforcing the concept of the all-hazards approach. In addition, they provide some protection against system shutdown or reduced capacity due to deterioration and other potential causes of upset.

For many years, engineers thought about resiliency as the ability to bring a system back to where it was previously. For example, if a water intake was damaged, the engineer would typically think about repairing the intake. Now, the emphasis is shifting to the idea that the particular structure isn't important – it is the continuation of the *function* served by the infrastructure that is important. And, because the serviced community may be changed by the disaster itself, the damaged infrastructure may no longer be the best way to provide that function. Thus, if a water intake on a river were to be destroyed by an attack, it is not at all clear that the intake should be rebuilt – perhaps the city is no longer comfortable with river-supplied water and wants to switch to well-water; perhaps the size of the city's population has changed, or perhaps supply lines for coagulant have been disrupted so that river water is no longer feasible to treat. And, of course, disasters also allow new technology to be installed, simply because a capital outlay is required. Thus, if the intake were to be built, the pumping system would be re-analyzed and new pumping configurations and technologies are likely to result.

Another resiliency theme that engineers have been exploring is critical infrastructure interconnectedness. Under Homeland Security Presidential Directive 7 (http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm), the federal government designated 17 critical infrastructures and key assets in the United States which need protection, the water supply system being one of these. Work has proceeded in planning for resiliency in all these sectors (although it is difficult due to the much-publicized fact that 85% of our nation's infrastructure is privately owned) but engineers have realized that the resiliency of one sector effects that of another. In the example of this note, an attack on the electrical power grid would cause failure of water supply pumps, and failure of the water supply system would massive disruptions in the health care system, the fire protection system, and, more generally, the operation of daily business. Thus, there is much current effort on connecting models, simulations, and practice exercises across the full spectrum of infrastructures.

In conclusion, engineering generally looks at resiliency through an all-hazards lens and attempts to provide both mitigation and response mechanisms which will protect the functionality of the system and systems connected to it.