

Personal Perspective:

Program Management and Events of Scale^{1, 2}

Bob Prieto

Since early 2001, I have observed the impact of a series of high-profile events of scale. These events of scale have encompassed both manmade as well as naturally occurring events and the lessons outlined below are derived from a systems perspective and are to a large degree independent of the initiating event. Much has been written about individual events, the failures and successes in being prepared, the lessons learned in the immediate aftermath and the challenges during recovery.

This paper looks more broadly, focusing on programmatic features common in our preparation and planning to resist, respond and recover from these events. Careful consideration may improve our overall infrastructure resiliency and improve outcomes in the future. Table 1 summarizes my perspective in observing each of these events and to the extent possible the lessons learned have been grouped into three phases of resiliency:

- Resist phase
- Respond phase
- Recover phase

Clearly the list is not all encompassing but provides a starting point and framework for future development.

Where My Involvement Began

Maybe it was the high-altitude air and snow-covered mountains of Davos, Switzerland or perhaps the eclectic collection of people from around the world that inspired nobler ideas. But whether from within or without, I came to a crossroads that very much changed how I thought about many things in life. How I perceived the world, or more specifically the infrastructure systems that enabled the day-to-day functioning of the world we live in, changed in several fundamental ways.

That day was January 26, 2001 and the Governors of the Engineering & Construction community of the World Economic Forum were due to have their annual meeting. Traditionally, this meeting was a time to renew global friendships and make new ones. But this day was different. We awoke to the

¹ Second Editions are previously published papers that have continued relevance in today's project management world, or which were originally published in conference proceedings or in a language other than English. Original publication acknowledged; authors retain copyright. This paper was originally published in *PM World Today* in July 2008. It is republished here with the author's permission.

² How to cite this paper: Prieto, R. (2008). Personal Perspective: Program Management and Events of Scale, Second Edition, *PM World Journal*, Vol. IX, Issue V, May 2020. Originally published in *PM World Today*, July 2008.

news that Gujarat, India, had experienced a terrible earthquake the night before, with widespread failures in buildings and supporting infrastructure.

We also awoke to find one of our members from India exhausted from a sleepless night on the telephone trying to mobilize the heavy equipment and other resources he had to respond to this horrific tragedy and to his anger and frustration that “doing the right thing” was hampered by the lack of an efficient way for these new first responders, engineers and constructors, to engage with the public sector.

Table 1	
My Perspective during Events of Scale	
Event	Perspective
Gujarat, India Earthquake	World Economic Forum Engineering Governor
9/11	Chairman \$1 billion NYC headquartered engineering firm Co-chair NYC Partnership & Chamber of Commerce Infrastructure Task Force
SARs	APEC Business Advisory Council (US representative appointed by President)
Tsunami	Co-founder Disaster Resource Network APEC Business Advisory Council (US representative appointed by President)
Bird Flu	APEC Business Advisory Council (US representative appointed by President)
Supermarket Fire, Paraguay	Co-founder Disaster Resource Network
South Asia Earthquake	Co-founder Disaster Resource Network
Hurricane Relief, Grenada	Co-founder Disaster Resource Network
Katrina	Co-founder Disaster Resource Network Fluor served as FEMA response contractor for public assistance and temporary housing

It was out of this frustration and perhaps the thin air of the Swiss mountains that the Disaster Resource Network (originally called Engineers without Borders in those early days) or DRN was first conceived. Later we were to come to learn that at the same time in another hotel in Davos, the Transportation and Logistics Governors were arriving at the very same conclusion.



The **2001 Gujarat earthquake** was the most devastating earthquake in India in recent history. It occurred at 0317 hrs GMT, on January 26, 2001, which coincided with the 51st celebration of Republic Day (India). The location of the epicentre was Bhuj (23.6° N 69.8° E) Gujarat, India. The earthquake measured 7.9 on the Richter scale. At least 20,005 people killed, 166,836 injured, approximately 339,000 buildings destroyed and 783,000 damaged in the Bhuj-Ahmadabad-Rajkot area and other parts of Gujarat. Many bridges and roads were damaged in Gujarat. At least 18 people were killed and some injured in Southern Pakistan. The quake was felt throughout Northern India and much of Pakistan. It was also felt in Bangladesh and Western Nepal.

The private sector has critical skills that can prove vital in the aftermath of a disaster: engineering skills to probe collapsed buildings; logistical skills to transport and distribute supplies; technology skills to recover vital data and restore services; and above all, management skills to help organize all of the above. However, getting these skills where they are needed when they are needed is a formidable undertaking. This is the role of the DRN, to create a resource network that can be quickly mobilized in the wake of a disaster.

Over the years the DRN has added value where it can and as a co-founder of the DRN and a board member I have had the opportunity to consider many of the lessons learned from other disaster's where we have been able to provide assistance.

The need for such a clearinghouse was only reinforced by the terrorist attacks of September 11th and in February 2002 the DRN was formally launched by the World Economic Forum (WEF).

September 11th: My Programmatic Focus Begins in Earnest

I was in New York on September 11th 2001, and at the time serving as chairman of the city's largest engineering firm and active in a number of the professional and business groups that bound the engineering and construction industry tightly to the fabric of the city. As the attacks unfolded, our response as a company and an industry began. I am proud of what we did and what we were able to achieve during those early minutes, hours and days but remain uncertain about whether we lost the opportunity in the recovery phase that such a disaster offered.



Many of the key thoughts and observations that follow in this paper draw on my experience as a New Yorker, one who grew up and worked in the city throughout his entire career and who served as co-chair of the Infrastructure Task Force established by the New York City Partnership in the aftermath of the September 11th attacks. They also draw on a dimension which lay hidden until the aftermath of 9/11, namely as a student of the history of great engineering “system” failures.

It was only in relatively calmer moments after those first few weeks that I realized what we had started in Davos, namely linking business more tightly into large scale and systemic disaster response, was the right thing to do. It was also during this period that the notion of the three phases of resiliency (3R’s) first began to develop in my own mind.

In essence, I believe now, as I did then, that history has handed our profession an unusual challenge as well as an unmatched opportunity. How we respond will say much about the future of the heavily engineered environment we call our cities as well as much about our own profession. Our ability to provide effective and true program management for the broad array of infrastructure systems which underpin the daily activities that we take for granted will rest very much on our ability to embrace the lessons of history at their most fundamental level.

ABAC Experience

During the period of January 2003 to January 2006 I had the opportunity to serve as one of the three US representatives to the Asia Pacific Economic Cooperation (APEC) Business Advisory Committee or ABAC. This position was held by three business leaders from each of the 21 economies that then comprised APEC. The role of ABAC was to advise the leaders of these 21 economies as well as the US administration on broad regional economic barriers, challenges and opportunities. This was a

group whom I had interacted with dating back to shortly after its inception and one where my focus had traditionally been around the issues of infrastructure development and the ability to practice engineering in each of the region's economies.

Over time, the experience from my involvement in co-founding the DRN and my attention to how could we learn from the events of 9/11 took my thinking and actions within this forum in some different directions. There were many drivers to this shift in personal focus but the events in the APEC economies themselves were enough of an impetus.



While 9/11 was an APEC event, in all honesty I'm not sure it was thought of that way, at least not until the security requirements which emerged began to bite into the ability to efficiently move goods and people. If nothing else, APEC was about trade and business and on these, 9/11 had an impact.

But it was really other events that drove the point home - that events of scale had regional if not global impacts and more importantly for me, the kind of infrastructure systems that they challenged were broader than what I had first considered after Gujarat or 9/11. My perspective from these earlier events, which by this time was fully a systems perspective, caused me to step back and look at some of the system vulnerabilities and challenges that APEC faced, as well as how the lessons learned that I was able to articulate after 9/11 might apply. Additionally, this new perspective caused me to consider what might be learned from some other large scale system failures and to try to articulate these lessons learned as part of a more comprehensive perspective.

In many ways this paper is about trying to share this work with others who are charged from a programmatic perspective for planning and implementing the systems that will be required to deal with the future's unknown events of scale.

Let me turn just for a second to the APEC situation, though. History has shown that APEC is vulnerable to severe economic shocks especially those associated with these so called events of scale. Examples include:

- Man-made
 - 9/11
- Environmental
 - SARS
 - Bird Flu
- Natural
 - Earthquake
 - Tsunami

In many ways APEC is the most vulnerable region in the world to these broad impacting events of scale with:

- 60% of the World's Population
- 9 of the 10 Largest Earthquakes of Last Century
- 8 of the 10 Deadliest Tsunami's in History
- All 8 Major Typhoons of Last Century

The Three Phases of Resiliency (3Rs)

The resiliency of large systems can be thought of as encompassing three temporal phases associated with any event of scale. These three phases include: the Resist Phase, or the period of time which precedes the occurrence of an event of scale and more importantly that period of time when actions can be taken to mitigate the impacts directly associated with the event itself; the so called Respond Phase; and the ability to efficiently recover or the Recover Phase. These three phases are independent of whether the event of scale is man made or naturally occurring to a very high degree. In each phase a true "systems" perspective is required. Later in this paper I will summarize lessons learned by each of these phase to help those planning and managing large complex programs consider the risks and management principles which they should be considering at a program level.

September 11th – The Beginning of My Program Perspective on Events of Scale

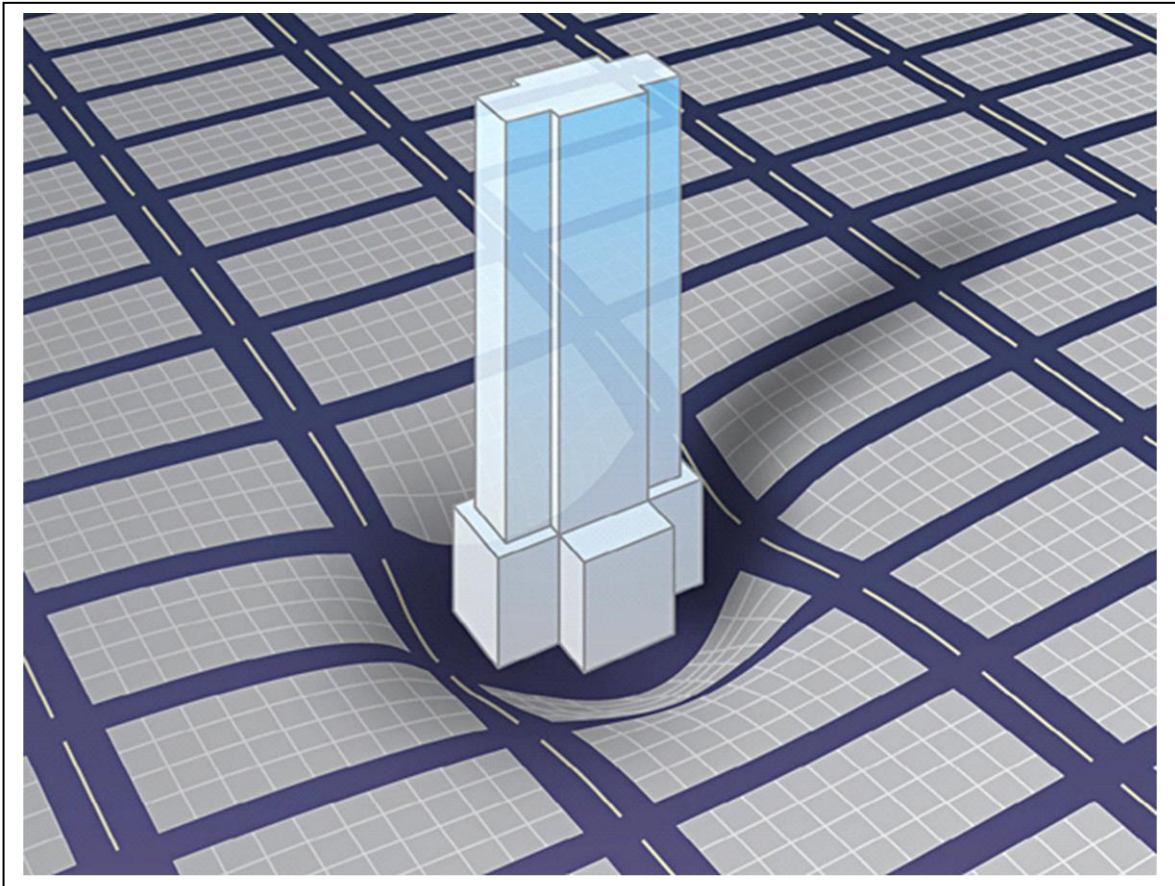
September 11th provided the personal impetus to think about some of these broader lessons learned, and while developed initially around a singular event of scale, their relevance has continued to ring true in each subsequent event.

What are those lessons learned?

Lesson #1 – Link between infrastructure and development is highlighted

I sometimes feel this has been a hobbyhorse of mine for too long. Infrastructure and development are intricately linked, often in ways we fail to fully appreciate. Each is the sine qua non of the other. Each of these "systems" is tightly coupled. However, as is often the case with all that we engineer, we can best appreciate the strengths, weaknesses and functionality only in their failure or application in response to some new paradigm.

September 11th highlighted the interrelationships of infrastructure and development. In the "localized" failure of "development" (the collapse of the World Trade Center Towers), we witnessed a "localized" destruction of the attendant infrastructure (1 and 9 subway, local power grid, PATH station at WTC, etc.). In the reconfiguration of "regional development" (an estimated 29,000 employees working outside NYC as a result of September 11th and another 29,000 temporarily backfilled in other existing metropolitan-area space), we reconfigured our "regional" transportation network (mandatory HOV, increased ferry service, increased transit ridership at other river crossings, etc.). Similar analogs exist for utility and telecommunications networks affected on September 11th.



However, this ability to reconfigure the infrastructure systems in response to a new development paradigm draws heavily from what we find in Lesson #2.

Lesson #2 – “Core capacity” of infrastructure systems is essential

At a point shortly after September 11th I had the opportunity to attempt to explain the importance of some planned New York City transportation improvements to members of the political arena. The basic case I tried to make was that these improvements were about enhancing the “core capacity” of a well-developed transportation network in order to improve overall system reliability, availability and performance. By “core capacity” I’m referring to the degree of interconnectivity of the various elements of the system, as well as the number of alternative paths available...its flexibility and redundancy.

De facto, these additions to “core capacity” strengthened the overall system, going well beyond the benefits associated with new system connections from some new point “A” to new point “B.” Traditional project evaluation models focused on “new riders” from new connections between points “A” and “B.” But, in complex systems, the dislocations that can be caused by even a partial loss of overall system capacity and capability can be much more profound. Similarly, the improved reliability, availability and performance created by adding “core capacity” to a complex system can pay dividends not often easily seen.

Such was the case for the regional transit system in the aftermath of September 11th. The “core capacity” of these systems provided the flexibility to deal with commuting patterns literally modified overnight with lines and stations outside the immediately affected area, seeing changed passenger volumes exceeding those often associated with new point “A” to “B” connections. It was gratifying to receive the call from the political arena several days later stating that they now understood “core capacity.”

Each of the infrastructure systems impacted by September 11th responded more or less quickly depending on the “core capacity” inherently incorporated in the system as well as the concentration of “critical infrastructure” in the damaged area. Older systems tended to be more “built out” while many newer systems were still heavily focused on building new “A” to “B” connections and as such had not yet achieved the level of “core capacity” of some of the more mature systems. This suggests that “core capacity” needs to be a criterion as we plan and implement the new infrastructure the 21st century will undoubtedly require.

Complex systems need a new model. We must recognize that dislocations can be profound. We must also recognize that improved reliability, availability and performance pay hidden dividends.

“Core capacity” is not just about the extent of a system or the number of alternate system paths. It is also about the intrinsic “quality” of the system at the point in time when it is stressed. This brings us to the third lesson learned.

Lesson #3 – Deferred maintenance represents a real cost and a real risk

The history of our profession is marked by exciting breakthroughs, great works of master builders, and outstanding service to our nation’s and the world’s population. Regretfully, it is also marked by the systemic degradation of some of our greatest achievements. As a society, and perhaps even in some parts of our profession, we do not see sustained maintenance as important as the creation of the next new grand work. Whatever the reason – its routine nature, the ability to hopefully do it tomorrow, the lack of technical complexity, or just plain lack of “sex appeal” – we are collectively guilty of allowing some of our most complex systems to fall into disrepair and to have their level of reliability, availability and operational and safety performance degraded. We have seen this most notably in failing rail systems in England and the U.S., but the impacts of deferred maintenance affect every element of infrastructure.

To a large measure, the ability of New York City’s transit system to respond and to fully take advantage of the “core capacity” inherent in its system has its roots back to the time of the system’s nadir. Out of crisis emerged a commitment to fund, reorganize, rebuild, improve and maintain to a well-defined standard. This, too, stands as one of the lessons to recognize as we engineer and operate our increasingly complex infrastructure systems. The strength of a well-maintained system is clearly seen in the aftermath. Other elements of infrastructure with higher backlogs of deferred maintenance are struggling to keep up and for many the challenges are in the years immediately ahead.

The condition of the system, how well it is maintained, is critical to sustain its ability to respond. The backlog of deferred maintenance should be viewed as an element of systems risk. On September

11th, and in its aftermath, systems in a “state of good repair” fared better in both the response and recovery phases.

This ability to respond often to other than design basis events is key to the integrity of “new” security and “safety” systems.

Lesson #4 – Operational and emergency response training is an integral element of critical infrastructure response

I won’t belabor the point since in many ways I’ve made it in looking across the prior three lessons. Succinctly, in the same way we factor constructability reviews into our design process and maintainability considerations into our construction details, so must we address operational training as an element of our engineering of critical infrastructure. The events of September 11th show many areas of exceptional performance, but this serves to only underscore the importance of operational training. The operational training for the events of the 21st century changed after September 11th. New scenarios need to be considered. New threats in the form of weapons of mass destruction, higher risk of collateral physical and economic damage and more extended response timeframes need to be addressed. First responder training (actions, interactions, communications, decision making) needs to be integrated with infrastructure system operational training.

Simple items such as establishing evacuation routes and off-property staging areas must be clearly provided by the infrastructure of our “built environment,” but also must be clearly integrated in first responder protocols.

Scenario training must be evolutionary as new threats emerge. Emerging response plans must be reviewed regularly and revamped as needed. Unusual incident reporting must be similarly kept up to date and relevant. Training to handle a growing range of threat scenarios must be kept current.

On September 11th we saw the impact of having the Emergency Operation Center (EOC) in proximity to a high-profile target. We also saw the importance of having safe, redundant capability and comprehensive integration with other relevant EOCs. Quick response is essential and the importance of interoperability of first responders has not received as much attention in the past as might be currently warranted.

But we must not stop there. We must also understand how the first responder team has evolved in light of our increasingly “engineered” environment.

Lesson #5 – Today’s highly engineered environment requires a first responder team that goes beyond the traditional triad of fire, police and emergency services

In early 2001, as I sat in the Engineering & Construction Governor’s meeting of the World Economic Forum (WEF) in Davos, Switzerland, I saw, with great frustration, the importance of the role of the engineer and constructor as part of a new first responder team. Out of that frustration grew the WEF DRN.

On September 11th we witnessed the engineering and construction industry voluntarily reach out and provide the technical and construction expertise for one of the greatest disasters in a highly engineered environment. All necessary protocols were not firmly in place and response training had

never fully factored this dimension in. Yet, this “fourth responder” will be even more critical as the 21st century unfolds.

While many good examples do exist, response protocols in our “engineered” urban environment will increasingly need to proactively incorporate this “fourth responder.” New, dedicated first responder training facilities reflecting the unique nature of highly “engineered” environments and their infrastructure need to be deployed, and legislation provided to remove the onerous risks that accrue to engineer “volunteers” who are often not covered by Good Samaritan statutes.

If we learn – and remember - each of these five lessons well, we will greatly enhance our abilities to resist and respond. But this must also be matched by our ability to recover.

We design to resist, to avoid, catastrophic failure in our critical infrastructure, to delay the failure as long as possible if it’s not preventable, and to minimize loss of life, collateral damage, and degraded system performance. Having built in as much resistance as makes sense from a risk-weighted and operational and economic perspective, we enhance our ability to respond. We provide “core capacity”; we focus on reliability, availability and performance. We reconfigure inherently resilient systems for both the short- and the long-term.

But, for our critical infrastructure, that is not enough. We must recover the capacity and service that was destroyed. We must restore the “engineered” fabric, making it better than it was, if possible. We must engineer for recovery. From an engineering standpoint, this can mean many things:

- Providing for accessibility to the sites of “critical infrastructure”
- Ensuring availability of specialized construction equipment, contracts and materials
- Developing a well-documented system with clear interface points
- Preplanning and rehearsing response and recovery scenarios for high-probability events (earthquake, hurricane, flood in areas so prone)

Together, these lessons from September 11th provide our program managers of large infrastructure systems with a solid foundation. But even more lessons must be learned.

Be SMART: The New Vulnerabilities

The vulnerabilities of September 11th do not represent the full range of threats the future may hold for our critical infrastructure. The attraction to public infrastructure as a likely target is driven by the political statement it makes, the potential for destabilizing public confidence as well as the international recognition associated with higher profile targets. By its nature, infrastructure is an open system. Its accessibility is predictable, its demographics known and its behavior on a diurnal basis well established. It provides a target that by its very nature can cause maximum harm.

But its vulnerability, or more broadly society’s broad vulnerability, is not limited to man-made events but rather extends to natural phenomena as my subsequent observations as a DRN board member and a member of ABAC unfortunately showed me time and time again.

We must be SMART about these vulnerabilities. We cannot eliminate or avoid them. But if we heed the lessons of history, we can learn from them and mitigate their consequences.

These SMART vulnerabilities may be broadly grouped into five areas:

- Systems
- Maintenance & Operations
- Attitude
- Risk Taking
- Transitional

The challenge is to build on the “lessons learned” on September 11th as previously described and to also consider other large-scale, “systems” scale, events.

Consideration of each of these vulnerabilities and the lessons learned within the framework provided by the 3Rs provides a basis for reviewing the adequacy of existing infrastructure systems and planning their enhancement. They provide a framework for truly getting “value for the money.”

Let’s look at each of these five types of vulnerabilities.

System Vulnerabilities

The events of September 11th drive us to take a “systems perspective” when reviewing our critical infrastructure. Not surprisingly, the first set of vulnerabilities we need to be SMART about deal directly with the very nature of the system.

In particular, we need to understand and learn from the risks associated with:

1. Failure to recognize the “built environment” as a growing and ever more complex system
 - a. This is perhaps the most fundamental risk we have. Development and infrastructure do not exist in isolation.
2. Inadequate “system” understanding
 - a. It may not be “rocket science”...or a high-technology defense system...but it is no less important to understand what may go wrong, and how to detect and remedy it.
3. Positive feedback loop risks
 - a. Also described as “progressive” failures, these considerations affect everything from the structural systems of a building, such as we saw induced by fire in the World Trade Center, to feedback mechanisms that degrade other elements of the “system.” This was seen in the need to relocate the Emergency Operations Center located at 7 World Trade Center.
 - b. This was also seen in the health related events of scale that struck the APEC region and crippled the very first responders who were in increasing demand.

4. Centralized control weaknesses in complex systems
 - a. There is a need for “interoperability” and an ability to “see” the situation. Partial decentralization of systems is required.
 - b. This was an issue faced in the Gujarat earthquake that impeded the initial movements of heavy equipment.
 - c. This was also seen in the APEC health crisis where economies initially affected tried to control information flow further abetting the spread of these diseases.

5. “Tight Coupling” of systems
 - a. Simply put, an event in one system leads to an event in another in short order. This was previously detailed in “Lesson #1.”
 - b. The health crisis in APEC impacted broader economic performance as business travel became an undesirable risk.

6. Failing to KISS
 - a. No, this is not the romantic in me, but rather the importance of “Keeping It Simple...Stupid.” We must recognize some classes of systems and certain technologies are inherently open to chains of failure. In such systems, adding additional safety systems only raises the level of complexity.

7. Inadequate “core capacity”
 - a. Lesson #2 highlighted the importance of interconnectivity, flexibility and redundancy to system responsiveness to unplanned events. Core capacity was a major factor in New York’s transit systems being able to restructure themselves immediately following September 11th.
 - b. All too often we emphasize “reach” (new customers) over “responsiveness” when making key decisions regarding our infrastructure investment.
 - c. The tsunami that impacted the Indian Ocean struck many areas where infrastructure coverage was limited at best before this event of scale.

Consideration of these vulnerabilities will enhance the resiliency of critical infrastructure. Those systems that more fully addressed these considerations responded better on September 11th.

Maintenance & Operation Vulnerabilities

If “system” vulnerabilities focus on ensuring that the right system is put in place, then “maintenance” vulnerabilities are focused on keeping it that way.

Specific risks to learn from include:

1. Failing to recognize the importance of “state of good repair”

- a. We saw this in Lesson #3. Those infrastructure systems in a “state of good repair” suffered less collateral effects when a portion of the system was stressed to failure.
 - b. There will be a tendency to compensate for maintenance and operational vulnerabilities by adding on top of the existing base system. In complex systems, in particular, this can act to create new risks. The “foundation” must be strong.
2. Inadequate renewal of emergency training
 - a. The systems of our “built environment” are not static, nor are the threats they face. Emergency training must be undertaken recognizing the dynamic environment within which our “built environment” exists as well as its own inherently dynamic nature.
3. Inadequate operating provisions to limit disturbances
 - a. Failure must be contained or “localized” to prohibit “tight coupling” effects from taking hold. In New York, on September 11th, we saw operating action take preventive steps against further failure of the PATH and NYC Transit lines as a result of flooding in damaged sections. In more routine circumstances we find good examples in power-grid inter-ties.

Attitude Vulnerabilities

In contrast with system and maintenance vulnerabilities that focus on whether the right system is in place and whether it’s sustained properly, attitude vulnerabilities address our willingness to accept an unexpected or undesired “truth.” Specific “attitude” risks include:

1. Cognitive Lock
 - a. In life, particularly when we are under stress, we expect certain situations to evolve in certain ways. Sometimes they don’t. Cognitive lock occurs when we hold onto a course of action against all contradictory evidence. This can be particularly disastrous when combined with a complex system and often requires a fresh pair of eyes to see the new “truth” in front of us. I include haste as an attitude vulnerability given the risks often incurred, unknowingly, when blindly charging ahead.
2. Over-commitment to bureaucratic goals
 - a. The goal has been set and any deviation from the goal is not acceptable. Problems that arise are ignored if they put the goal at risk. The “unmovable” goals set for aviation security ignored the realities of having a comprehensive approach in favor of meeting a fixed end date. Does mere achievement of the bureaucratic goal ensure we have accomplished our true aim?
 - b. Was failure to use available government owned housing that was larger than the FEMA spec an acceptable decision in the early days after Katrina?

3. Prisoner to Heuristics

- a. Past experience or what we've heard prevents us from taking a broader look. We adopt a perspective of "it never happened, so it's not credible." When the command center was established at the World Trade Center on September 11th, it was set up in the shadow of the unstruck south tower. The possibility of a deliberate attack on two (or more) buildings at the same time in a way designed to cripple first responder capability was not considered credible.
- b. Being a prisoner to heuristics also involves a failure to consider what we see or learn from analogous systems or settings. Are multiple, simultaneous attacks or attackers on first responder teams the new norm? Or do we run the risk of the next attitude vulnerability?

4. Denial

- a. Conventional threat analysis has us consider a range of "likely" scenarios and design our systems to resist, respond and recover from such scenarios. But the "unlikely" is also possible and it, too, must be considered. How do you address these "unlikely" scenarios in your system design and operation? At one level you can't because one can always postulate another "unlikely" scenario that will defeat any specific system measures you undertake. So what is one to do?

In many ways this brings us full circle to the need to have inherently flexible, redundant and reliable systems. "Core capacity" provides the trained system operator with the tools to address a broad range of "unlikely" scenarios.

Contingency planning for our critical infrastructure must include training in the capabilities and limits of various system elements. The "unlikely" must be part of our planning processes.

5. Failure to learn "Lessons Learned"

- a. Over the last year I've tried to distill down the events of September 11th into a set of factors for us to consider in the future design and operation of our critical infrastructure. These lessons are not unique to the events of September 11th. Rather, from an engineering standpoint, we have seen many of these lessons learned in prior events of scale in heavily engineered systems.
- b. The interest in establishing proactive mechanisms in APEC for dealing with a broader type of events of scale was limited until the tsunami drove home the point that there was an important commonality between all events of scale.

Risk-taking Vulnerabilities

None of us likes to be wrong. But the way we perceive risks and handle mistakes affects the range of actions we are willing to consider when faced with extreme situations. Two particular risk-taking vulnerabilities are worth calling out.

1. Litigation constrains risk-taking in the “Respond” and “Recover” phases
 - a. All evidence points to the engineer and constructor increasingly being part of tomorrow’s first responder team in our heavily “built environment.” This was one of the lessons learned on September 11th. But while the engineering profession responded, voluntarily and overwhelmingly, it did so at its own peril. As licensed professionals undertaking their profession, it was not clear whether they were covered by Good Samaritan legislation. How will they behave next time if a lawsuit is filed for a “mistake” they made while trying to help others?
 - b. To what extent was litigation or the fear of public opinion a constraint in communicating early infections in the various APEC health crises?

2. Fear of “satisficing”
 - a. We are often called to make decisions or take actions in the absence of complete information. Our willingness to take action and move forward with an apparently workable solution is often a function of how mistakes are perceived and handled.
 - b. Running heavy cranes out across the “debris field” following the collapse of the World Trade Center was an example of willingness to “satisfice.” No as-builts existed and a high degree of judgment and risk-taking was required. How might we have handled a mistake that sent a crane toppling or crashing through the sub-basement structure?

Transitional Vulnerabilities

“Change” is the watchword of life. In the aftermath of September 11th, we will seek to improve what we do, add new levels of safety, change protocols, etc. But in the process we must recognize that complex infrastructure systems, and, for that matter, systems in general, are often most vulnerable immediately before, during and immediately after this change process. What are some of these transitional vulnerabilities and what must we be cognizant of as we move through these transition stages? They include:

1. Inadequate use of currently deployed resources
 - a. There is a tendency to look for the “silver bullet” as opposed to better deploying and applying the resources at hand.

2. Change processes further stress existing systems
 - a. These risks are today’s issues as we modify our air travel regimes, handling of “just-in-time” commerce and revamp first responder efforts. Change for change’s sake is not necessarily the answer and, approached narrowly, may increase the overall risks we face.

3. New system failure rates not planned
 - a. True operating characteristics and failure rates of new systems can only be understood after an extended period of operating under both good and bad conditions. The old adage that you “don’t know what you don’t know” is particularly relevant during a transitional period.
4. Technology put ahead of people
 - a. September 11th taught us that people cannot, and should not, be taken out of the loop. It was individual actions that led to the shutdown of transit lines....not technology. It was individual action that dispatched ferries, busses, generators, cranes and engineers...not technology. Technology is a powerful enabler of people...but it needs to fit them, not the other way around.

**Case History:
Hurricane Relief**

- ◆ Needs Addressed:
 - Hand tool kits for debris removal and temporary repair of 90% of houses damaged
 - Chainsaws, safety goggles, rope, tree branch loppers
 - Line of credit to repair damaged college
- ◆ Lesson Learned: Provision of “tools” to facilitate self-recovery at earliest possible date is a best practice

FLUOR

17

Concluding Thoughts

I’ve looked back at some of the lessons we should learn from September 11th as well as other events of scale from my DRN and APEC perspectives as well as looked around at what experiences from other “systems” failures have taught us so we may better understand the full range of vulnerabilities our critical infrastructure faces. But what are the challenges ahead? That is the real question and why we must truly understand the programmatic challenges that planning and responding to events of scale requires.

Check List for 3Rs

Resist Phase Lessons Learned

- Requirements for resistance/reduction of impacts from events of scale
 - Long term, strategic view
 - Recognized interdependencies
 - Proactive action/planning
 - Improved communication across bureaucratic “silos”
 - Recognition that an event of scale exists that will overwhelm all measures
- Establish Non-Government Organizations (NGO) linkages/protocols
 - UN Disaster Relief, International Red Cross
- Identify supporting business resources and put outreach mechanisms in place
- Provide pool of expertise to assist in response phase planning
 - Identify protocols required
 - Facilitate mitigation of barriers
- Understand those systemic needs best met by business
- Understand special needs unique to the each potential event of scale
 - Know what may be quickly mobilized and sources

Case History: Earthquake

- ◆ Needs Addressed:
 - Air transport of 60 Tons of Red Cross medical supplies
 - Air transport and distribution of 1000 tons of food
- ◆ Lesson Learned: Need for Airport Emergency Team



FLUOR

16

- Create a common definition of “Critical Infrastructure”

Critical Infrastructure Defined

- Systems whose rapid failure would lead to a catastrophic loss of life
- Systems whose failure or significant degradation would lead to unacceptable economic consequences
- Systems whose rapid failure would significantly impact rescue and response efforts
- Systems whose significant degradation would significantly impact recovery efforts

NOTE: Rapid is relative to the consequences possible as opposed to an absolute timescale.

- Recognize “Core Capacity” of infrastructure systems essential
 - Core Capacity
 - Degree of interconnectivity of various elements of a system
 - Number of alternative paths available
 - Flexibility and redundancy
 - Traditional project evaluation models have rewarded new connections vs. responsiveness and reliability
 - Deferred maintenance = real cost, real risk
- Operational/emergency response training essential
 - Need to reconfigure “First-Responder” team
- Complex systems require a new model
 - Dislocations can be profound
 - Improved reliability, availability and performance pay hidden dividends
 - “Quality” of the system counts
 - Critical to sustain ability to respond
 - Backlog of deferred maintenance should be viewed as element of systems’ risk
 - Systems in “state of good repair” fared better in both response and recovery phases
 - Key to integrity of “new” security and “safety” systems
- Operational training integral to engineering of critical infrastructure
 - Establish evacuation routes and off-property staging areas
- Scenario training must be evolutionary as new threats emerge
 - Review existing emergency response plan
 - Revamp unusual incident reporting
 - AFT Bomb Threat Training
- Emergency Operation Centers must be safe, redundant and integrated with other relevant EOCs
 - Quick response essential

- Interoperability of First Responders
- Role of the Engineer and Constructor is redefined
 - The New First Responder
- Engineer for recovery
 - Provide for accessibility to the sites of “Critical Infrastructure”
 - Ensure availability of specialized construction equipment, contracts and materials
 - Develop a well-documented system with clear interface points
 - Pre-planning and rehearsing response and recovery scenarios for high probability events (earthquake, hurricane, flood in prone areas)
- Failure to recognize the “built environment” as a growing and ever more complex system
- Inadequate “system” understanding
 - What may go wrong, how to detect and remedy
 - Positive feedback loop risks
 - “Progressive” failures
 - Centralized control weaknesses in complex systems
 - Need for “interoperability”
 - Need to “see” the situation
 - Partial decentralization of systems required
 - “Tight coupling” of systems
 - An event in one system leads to an event in another in short order
 - Failing to KISS
 - KISS – Keep It Simple Stupid
 - Some classes of systems/technology are inherently open to chains of failure
 - Adding safety systems only raises level of complexity
 - Inadequate “Core Capacity”
 - “Reach” emphasized over “responsiveness”
- Failing to recognize importance of “state of good repair”
 - Tendency will be to “add” on top of existing base “system”
 - The “foundation” must be strong
- Inadequate renewal of emergency training
- Inadequate operating provisions to limit disturbances
 - Good example – power-grid inter-ties
 - “Cognitive lock”
 - Holding on to a course of action against all contradictory evidence
 - Disastrous when combined with a complex system (Fermi accident is example)
 - Requires a fresh pair of eyes
 - Haste
 - Poor quality control on slag inclusions did more to sink the titanic than the iceberg

- Over commitment to bureaucratic goals
 - Growing problems ignored for sake of meeting goals
 - Congress and TSA on aviation security (NASA and Morton Thiokol is example)

- Becoming a prisoner to Heuristics
 - Broader look constrained by...
 - Past experience (never happened so not credible)
 - What we heard (often narrow and limited)
 - Failure to consider lessons learned in analogous settings or system
 - Denial
 - Failure to consider the unlikely
 - Absence of contingency plans for future
 - Failure to learn “lessons learned”

- Inadequate use of currently deployed resources
 - “Silver Bullet” syndrome

- Change processes further stress existing systems
 - Air travel
 - Just-in-time commerce
 - Seaport security
 - Border crossings
 - First responders

- New system failure rates not planned
 - Don’t know what you don’t know
 - Systems must be learned under good conditions and bad
 - Technology Put Ahead Of People
 - Technology needs to fit people – not the other way around

- Scale matters
 - Both a Challenge and an Opportunity

- Our cities –development and infrastructure –must be designed for the 3Rs:
 - Resist
 - Respond
 - Recover

Checklist for 3Rs

Respond Phase Lessons Learned


- Quick response with the right resources can limit immediate and longer term impacts from events of scale but requires:
 - Mobilization of all sectors of society
 - Government, Non-Government Organizations (NGO), Business
 - Clear understanding of systemic issues and resource needs required in response phase
 - Protocols in place, systems and structures for non-traditional interaction between sectors
 - Clear understanding of resources available
 - Exit strategy
 - Recognition that an event of scale exists which will overwhelm all measures

- Recognize that fast paced Government-Business interaction in a multi-national context will not occur
 - Government will default to major NGOs
 - Business resources best delivered through NGOs
 - NGO interface with business currently limited – focus needed

Case History: Tsunami

- ◆ Needs Addressed:
 - Airport Emergency Team (AET) deployed day after at request of UN Joint Logistics Center
 - Directed movement of all relief supplies arriving at Colombo
 - 177 flights per day
 - 6000 tons moved in first two weeks to 1,000,000 affected people
 - Broader appeal launched for food, water, shelter, field sanitation and medical services

- ◆ Lessons Learned:
 - Need to establish rules of engagement (have a plan)
 - Need for handover plan to build local operational capacity for logistical management of supplies
 - Need to extend concept to engineering, communication and other fields
 - Need to have broader pool of individuals trained in emergency operations
 - Need to participate in "transition coalition with NGOs and Government to plan and prioritize economic recovery process"



18


FLUOR

- Provide quick mobilization to meet systemic needs
 - Generic drugs typically required including understanding storage requirements and shelf life
 - Air transport appropriate for disaster zone capabilities and condition
 - Airport Emergency Team to manage logistics at receiving airport and provide supplemental handling equipment

- Structural and construction engineers to assess damage and assist victim rescue and recovery
- Transport and logistics specialists with special training in disaster management
- Provide network to aid mobilization of special resources from Business
 - Vaccines, burn treatment supplies, water treatment, field sanitation, temporary shelter, hand tools for debris removal
 - Recognize that needs evolve throughout the response phase

**Case History:
Supermarket Fire**

- ◆ Needs Addressed:
 - Antibiotics, anesthetics and antifungals
 - Burn Treatment (292 people)
 - Pre-assembled medical mission kits
 - Respirators and other medical equipment
 - Immediate air transport of above supplies
- ◆ Lesson Learned: Need for alert mechanism as specific pharmaceutical needs changed



FLUOR

15

- Prioritize requests to Business to match resources with needs
 - Avoid overwhelming the supply chain with lower priority supplies
- Establish handover plan to revert temporary management activities to Government
 - Know when to leave and have planned exit strategy
 - Stay close to Government immediately after handover from the Response phase to ensure no gaps develop
- Recognize need for alert mechanism as specific pharmaceutical needs changed
- Recognize need for Airport Emergency Team
- Establish Business response networks::
 - Need to establish rules of engagement (have a plan)
 - Need for handover plan to build local operational capacity for logistical management of supplies
 - Need to extend concept to engineering, communication and other fields
 - Need to have broader pool of individuals trained in emergency operations
 - Need to participate in “transition coalition with NGOs and Government to plan and prioritize economic recovery process

- Apply “Cognitive Lock” and “Heuristic” concerns in this phase as well
- Realize litigation constrains risk-taking in “Respond” and “Recover” Phases
 - Inadequate Good Samaritan Legislation for Engineers and Constructors
- Avoid “Satisficing”
 - Satisficing – A workable and fast-acting solution without complete information
 - Driven by how we “handle mistakes”
- Plan B needed for first line responders
 - Activation procedure for second line responders required
 - Rapid deployment of medical care services top priority
 - Accurate medical supplies procured through pre-arranged activation procedure with pharmaceutical companies
 - Established relationship with locals linking to local authorities and network
 - Quickly identify locations for medical centres
- Critical Supplies
 - Water
 - Food (Culture factors)
 - Temporary shelters
 - Clothing (Culture factors)
 - Medicines
 - Equipment (Heavy)

Checklist for 3Rs

Recover Phase Lessons Learned

- Successful recovery is possible but requires:
 - Long term vision of “success”
 - Transparency in implementing the recovery program
 - Focused effort on sustaining “reservoir” of good will
 - Recognition that Business plays unique role in post disaster economic recovery process through job creation

- Continue communication between Business and Government to ensure reservoir of goodwill not drained

- Insist on a transparent and corruption free Recovery phase

- Help prioritize economic recovery process

- Provision of “tools” to facilitate self-recovery at earliest possible date is a best

- Set requirement for a comprehensive and integrated systems view
 - Development and urban infrastructure
 - Consider all views: User, Operator, Regulator, Provider

- Remember the Four-Dimensional Framework
 - Extends below ground
 - Underground transportation arteries, etc.
 - Plans for changes with time
 - Adaptable buildings and infrastructure
 - Understand our engineered environment
 - Not only past and present;
 - More importantly—future
 - Understand how it will evolve
 - Understanding how 3Rs will be built in as system expands
 - Have a vision

References

"Disaster Response in APEC – A Unique Opportunity." APEC Business Advisory Council Business Summit. Mexico City. 22 February 2005.

"Handling the Unknown." Asia Inc. October 2003.

"Using the 3Rs to Deal with Crisis." Business Asia. June 2003.

"A 911 Call to the Engineering Profession." The Bridge, National Academy of Engineering. Spring 2002.

"The 3Rs: Lessons Learned from September 11th." Royal Academy of Engineering. 28 October 2002.

"The 3Rs: Lessons Learned from September 11th." The Russian Academy of Sciences. 17 March 2003.

"Urban Security: New York City as Microcosm." Journal of Technology in Society Elsevier Journals.

"Terrorism: Reducing Vulnerabilities and Improving Responses." Committee on Counterterrorism Challenges for Russia and the United States, National Research Council of the National Academies in cooperation with the Russian Academy of Sciences. 2004.

"Vulnerability of Public Infrastructure: A Systems Perspective." Homeland Security Summit. 6-7 June 2002.

"The Effect of 911 on the Engineering and Construction Industry." World Economic Forum Governors' Meeting for Engineering and Construction. New York, NY. 3 February 2002.

About the Author



Bob Prieto

Chairman & CEO
Strategic Program Management LLC
Jupiter, Florida, USA



Bob Prieto is a senior executive effective in shaping and executing business strategy and a recognized leader within the infrastructure, engineering and construction industries. Currently Bob heads his own management consulting practice, Strategic Program Management LLC. He previously served as a senior vice president of Fluor, one of the largest engineering and construction companies in the world. He focuses on the development and delivery of large, complex projects worldwide and consults with owners across all market sectors in the development of programmatic delivery strategies. He is author of nine books including “Strategic Program Management”, “The Giga Factor: Program Management in the Engineering and Construction Industry”, “Application of Life Cycle Analysis in the Capital Assets Industry”, “Capital Efficiency: Pull All the Levers” and, most recently, “Theory of Management of Large Complex Projects” published by the Construction Management Association of America (CMAA) as well as over 600 other papers and presentations.

Bob is an Independent Member of the Shareholder Committee of Mott MacDonald. He is a member of the ASCE Industry Leaders Council, National Academy of Construction, a Fellow of the Construction Management Association of America and member of several university departmental and campus advisory boards. Bob served until 2006 as a U.S. presidential appointee to the Asia Pacific Economic Cooperation (APEC) Business Advisory Council (ABAC), working with U.S. and Asia-Pacific business leaders to shape the framework for trade and economic growth. He had previously served as both as Chairman of the Engineering and Construction Governors of the World Economic Forum and co-chair of the infrastructure task force formed after September 11th by the New York City Chamber of Commerce. Previously, he served as Chairman at Parsons Brinckerhoff (PB) and a non-executive director of Cardno (ASX)

Bob can be contacted at rpstrategic@comcast.net.