Infrastructure Failures

Key Points

- Infrastructure is the network of utilities that supplies our basic needs for mobility, power, water, sewer and communications.
- This chapter covers major structural failures that are not triggered by some other hazard (e.g., an earthquake).
- Computer failure whether accidental or deliberate (e.g., cyberattack) is a form of infrastructure failure.
- The American Society of Civil Engineers (ASCE) gives the infrastructure of the United States an overall D grade and estimates it will cost $2.2 trillion to fix. The main concerns for Washington State are roads, bridges and mass transit.
- Many problems due to poor infrastructure are individually small but quickly add up, e.g., a vast number of small leaks causing some municipal water systems to lose up to 20% of their water during transmission.
- Infrastructure can be damaged during construction e.g., a contractor breaking a water main, or fail when new due to a design flaw, e.g., the collapse of the Tacoma Narrows Bridge in 1940. Not all infrastructure failures are caused by aging systems and structures.
- Occasionally, what is known about a threat to infrastructure becomes clear only after we build it. This has occurred with many bridges built in the early 20th century before Seattle was aware of the earthquake risk here.

Context

On August 1, 2007, the I-35W Mississippi Bridge in Minneapolis collapsed highlighting aging and vulnerable infrastructure across the United States. Many citizens began to wonder about the state of not just the bridges in their communities but also other critical infrastructure and buildings. This section addresses infrastructure failures of all types. Because power failures are especially complex, they are covered in their own section.

Most complex infrastructure is now controlled with computer systems (called supervisory control and data acquisition or *SCADA* systems). SCADA system failure is a type of infrastructure failure. There has been a lot of attention given to the threat of a cyber-attack on infrastructure system, especially the power system. The chance of a successful attack is very small, but the consequences would be very large if a successful attack did occur.

Examples of infrastructure failures include building collapses, water main breaks, gas pipe ruptures, dam failures, steam pipe explosions and related types of events. Recently failures in communications infrastructure have been added to this list.

Many of the problems are related to the age of American infrastructure. In many places pipelines, bridges and other structures are over 100 years old. Some systems in Seattle are approaching this age. The shear amount of investment it would take to upgrade all of it would be $2.2 trillion according to the American Society of Civil Engineers, which also assigned an overall D grade to the nation's infrastructure[i].

Locally, responsibility for Seattle's infrastructure rests with a collection of public and private agencies. Details of the systems and the agencies are given in the Community Profile.

Infrastructure failure is often felt as a secondary hazard to another incident such as an earthquake. While many of these primary hazards would damage even healthy infrastructure, the problem is compounded by weakened infrastructure.

While many problems of failing infrastructure are small scale and cumulative, this section concentrates on the upper end of the problem, large scale emergencies. Nevertheless, it is important to note that these large scale emergencies represent only part of a larger issue.

Replacing aging and inadequate infrastructure is costly and politically difficult. Without a clear crisis, it is a challenge to convince taxpayers to replace expensive structures. Nonetheless, some programs have been implemented and are addressing infrastructure improvement needs, e.g., the $365 million the Bridging the Gap levy.

History

The Seattle region has experienced some large failures, but none included major loss of life. This is a list of the major infrastructure failures in Seattle. In some cases, like the vault fires, the same events are dealt with in greater detail in another chapter.

November 7, 1940. Tacoma Narrows Bridge Collapse. One of the most famous infrastructure failures in the world occurred when a 42 mph wind caused the bridge to twist until its cables snapped. There were no casualties.

November 11, 1957. Sinkhole. A sewer line tunnel built in 1909-10 collapses, causing a massive sinkhole under Ravenna Boulevard. 10 families had to be evacuated. The system took two years to repair and cost $16,000,000 to repair (in 2013 dollars).

February 25, 1987. Husky Stadium Collapse. An addition to the northern deck collapsed during construction. The cause was the premature removal of six temporary wire supports that allowed the structure to sway too much. Workers noticed a support buckling and had time to escape, so there were no casualties.

November 25, 1990. I-90 Bridge Sinking. The bridge was under construction and not being used. It sank following a major windstorm. The pontoons that support the bridge had been opened to temporarily store water. The openings allowing additional storm water to enter.

July 19, 1994. Kingdome Ceiling Tiles. Hours before a baseball game, four large waterlogged tiles peeled from the ceiling and plunged into the seats. Two construction workers died in a crane accident during the repair. The cause was a badly leaking roof.

December 14, 2006. Drainage System. (Also in Flooding). Heavy rains overwhelmed the drainage system along Madison Street. Water built up in a valley in the street. It overtopped the curbs and rushed downhill, slamming into a home and killing one person.

May 2, 2007. Water Main Break Under University Bridge. A 24-inch main broke, causing a large sinkhole and worries about the integrity of the bridge abutment. The incident also damaged an 8-inch gas main and a conduit housing Qwest trunk lines. The bridge was not damaged, but water and gas service in the area had to be cut for most of a day.

January 19, 2009. Howard Hanson Dam. Engineers learned that parts of the abutment had a void. To reduce the chance of a catastrophic failure, dam operators would not be able to hold as much water in the reservoir, increasing the chance of flooding in the Kent valley. Temporary repairs were completed before a flood.

July 3, 2009. Fisher Plaza Data Center Communications/ Internet Outage. An electrical fire took Fisher Plaza data centers offline, bringing down several eCommerce sites including a credit card validation service. It was the third time Fisher had experienced downtime.

Likelihood

Infrastructure failures are unavoidable. Even if our entire infrastructure system was in top shape, there would still be construction accidents, operations errors, design flaws and unanticipated environmental issues. These failures occur every year, but these can be handled through daily business procedures. The question is how likely are major failures that precipitate large-scale emergencies? There seems to be an increase within the past 30 years, but this could be random variation or the result of earlier events being lost to history. Major infrastructure failures *seem* to happen very roughly once a decade on average but several can happen within a few years or decades can past without one.

The chance of a catastrophic infrastructure failure is much smaller than the failures described above. Most infrastructure failures are single-site incidents. Unless a single failure such as a dam failure or nuclear accident can affect a large area most infrastructure failures do not scale up to the catastrophic level. There are no dams in the City limits and Seattle is far from the state's only nuclear power plant in Eastern Washington.

SCADA systems make it theoretically possible to affect a whole infrastructure system at once. Despite the theoretical vulnerability, the world has never experienced a major computer-caused infrastructure failure. An attack is the most likely cause of cyber-induced infrastructure failure. Most analysts consider it a remote possibility because agents with the means (like states) lack the motivation to attack and those with the motivation (terrorist organizations) lack the means[ii].

Vulnerability

Seattle is the greatest concentration of infrastructure in the Pacific Northwest and one of the oldest settlements in Washington State. Seattle has a bigger collection of infrastructure maintenance needs than anywhere else in Washington State giving it an intrinsic vulnerability to infrastructure failure.

The vulnerability of individual systems varies greatly according to the condition of the components, system complexity, the ease and speed with which damage propagates through an infrastructure system and the amount of redundancy in the system.

Virtually every part of Seattle could be affected by one type of failure or another because of the ubiquity and dependence of every social and economic function on infrastructure. Some places are more sensitive than others, e.g., locations where multiple facilities or pipelines are co-located or where an area can only be serviced by one utility line, facility or transport route.

The most vulnerable periods in the life of a structure are during construction, right after it is built, and as it nears or exceeds it expected operational life. Most of Seattle's most dramatic failures occurred during one of these phases.

Many times, visible signs that are present before a failure allow people time to escape. Warning signs are the major reason there were no casualties during the collapse of the Tacoma Narrows Bridge, Husky Stadium, and the I-90 floating bridge.

Consequences

Infrastructure failures cause outages in whatever utility or service the broken structure provides. Most are single-site incidents. Infrastructure failures have caused fatalities, injuries and economic losses in Seattle and are expected to do so again. They are one of the most common secondary hazards where multiple sites could be affected. The scenarios below outline cases where the failure itself is the primary hazard.

The mostly likely infrastructure failure scenario would resemble past events. Many past failures have involved bridges and the water system. Failures are more frequent in systems under construction or in older components. Consequences would be worse if the failure occurs 1) in a heavily used or populated area and 2) the failed component is co-located with other key infrastructure. Finally, Seattle has a lot of infrastructure and therefore many potential failure scenarios.

A break in one of the 42" water mains was chosen as the Most Likely scenario because Seattle has had large water main breaks in the past, it is critical service and could cause significant 'collateral damage'.

There is no guarantee that the future will be a continuation of the past. The rise of networked SCADA systems fundamentally changes the nature of the infrastructure failure hazard because it is now theoretically possible to disable or even destroy a whole infrastructure network instead of mostly single-site failures. The chance of a catastrophic failure is currently considered very remote, but the consequences would be severe. The exact consequence profile depends on the infrastructure affected.

Most analysis highlights the power system as the greatest vulnerability in a modern urban environment. Following this work, a cyber-attack on the power system was chosen as the Maximum Credible Scenario even though there have been no such successful attacks to date and the chances of one are very small.

Most Likely Scenario

A 42" water main breaks near a bridge. The release of water undermines a bridge pier and co-located utilities (gas, sewer, and communications). There are no fatalities, but the area surrounding the collapse is impacted. Transportation corridors are affected. It impacts surrounding businesses and environment.

Category	Impacts 1 = low 5 = high	Narrative

Frequency	5	Infrastructure failures happen regularly. This scenario is similar to past events but with some added complexity that demands a higher level of coordination to manage consequences.
Geographic Scope	1	This is a single site incident although some impacts are felt outside the immediate area (e.g., utility outages).
Duration	2	The damage takes 2 days to repair. It takes an additional day for full service restoration.
Health Effects, Deaths and Injuries	1	There are no deaths or injuries as a result of the break.
Displaced Households and Suffering	2	Water and gas service to a school and nursing home is shut off. Nursing home residents have to be moved.
Economy	2	24 businesses are forced to close due to water damage.
Environment	2	The water main break undermines a sewer line breaking it. Untreated sewage spills into Lake Washington.
Structures	2	The water floods 5 buildings and undermines their foundations.
Transportation	2	The nearby bridge and streets near the break must be closed causing a temporary blockage. Fears are voiced about the effect of the water on the bridge but it is not damaged.
Critical Services and Utilities	2	The breakages of the water, gas and sewer lines force utility outages in the surrounding neighborhood. Public safety services are not affected.
Confidence in Government	3	The infrastructure is owned by the government. The public believes that it could have been better maintained.
Cascading Effects	2	The initial infrastructure failure leads to others and causes hazardous material (untreated sewage) to be released.

Maximum Credible Scenario

The world has never had a major cyber-attack, but in a first, an unknown group finds the motivation and overcomes major obstacles to mount a cyber -attack on the US power generation and transmission system. Operators take down computerized control systems but manual workarounds are not as efficient as computerized systems they replace. IT staff struggle for three weeks to bring systems back on line.

Category	Impacts 1 = low 5 = high	Narrative
Frequency	1	There has been only one confirmed case of a cyberattack destroying equipment, the STUXNET attack on Iranian centrifuges. Additionally some analysts doubt the motivation and/or capability of states or terrorist organizations to execute a paralyzing cyber-attack. Therefore, the frequency is given the lowest rating.
Geographic Scope	5	Vulnerable utilities are affected throughout the US.
Duration	4	Generators in the City Light and Bonneville Power Administration system are destroyed. Operators lose the able to control power management systems for three weeks causing blackouts and brownouts.

Category	Impacts 1 = low 5 = high	Narrative
Health Effects, Deaths and Injuries	2	5 people die due to the effects of power outages. They are involved in traffic accidents. 230 people become ill from eating spoiled food.
Displaced Households and Suffering	5	The extended power outages displace 1000s of people living in high rise buildings because water systems lack pressure to bring water to higher floors and the lack of power shuts down elevators. The transportation system is disrupted causing some food shortages. Schools close due to lack of power. Water is out in areas that require a pump until the pumps can be connected to a generator.
Economy	4	Most businesses in Seattle are forced to suspend or relocate operations outside Seattle. There is a surge in sales after the attack ceases partially offsetting lost business.
Environment	3	The attacks disable King County's sewage treatment plants. Untreated sewage has to be discharged into Puget Sound.
Structures	1	The attack does no damage to buildings but causes many to be temporarily inoperable.
Transportation	4	Traffic control systems are taken offline. The surface transportation system is heavily affected. Air traffic control systems continue to operate as do marine navigation systems.
Critical Services and Utilities	4	Multiple utilities are inoperable due to extended power loss and a lack of generators: communications, water, and power. Public safety is operating on manual systems which reduce capacity.
Confidence in Government	3	The public is initially sympathetic to the government but grows impatient as the outages continue.
Cascading Effects	4	Many control systems that prevent hazardous materials releases are offline.

Conclusions

Seattle has had infrastructure failures in the past and will probably continue to have them. As this community's infrastructure ages, it will require major investment to fix. Even if the maintenance backlogs are fixed, it is impossible to eliminate all design flaws, construction errors and operator errors. The big question is whether future incidents will be small or large.

Failures of single structures or sites can cause high numbers of casualties but have a limited geographic scope. Single failures can usually be contained relatively easily and recovery is fairly quick and complete.

Multiple failures or collapses could occur as a secondary hazard but are often so tied to the primary hazard than there is often no functional distinction. The major effect of an earthquake on the human community is structural collapse.

In the long run, the cumulative effects of all the small incidents related to aging infrastructure probably outweigh the effects of big, spectacular incidents. Much as chronic disease imposes a health burden on a community, chronically poor infrastructure imposes a socio-economic burden.

---

[i] New York Times. "U.S. Infrastructure is in Dire Straits, Report Says." 1/27/2009.
[ii] Clapper, 2013.