Digital Power

By Peter M. Curtis

Peter Curtis is the president of Power Management Concepts, LLC, in Bethpage, NY, and an associate professor at New York Institute of Technology.

The Perfect Storm on Steroids

Not every disaster is caused by nature

Will our growing reliance on all varieties of digital information coupled with the recent extraordinary natural disasters, deliberate assaults on IT infrastructure, and the increased obsolescence of the electric grid lead to the perfect storm on steroids?

In the first half of 2011 we have seen some erratic and catastrophic natural disasters around the world (see table 1). The disasters have affected and disrupted the lives of many.

Obviously, there have been natural disasters as long as the Earth has existed, but we have only been recording these events for about the last century or so. In addition, the number of recorded natural disasters is growing both nationally (see figure 1) and globally (see figure 2). With every day that passes, our critical infrastructures continue to expand, leaving us with more to protect. In our industry, we do take into account the natural environment, but our standards may need to be reevaluated based on new risk. The recent tornados, tsunamis, volcanic

Date	Location	Disaster
January 19th	Japan	Major volcanic eruptions
March 11th	Japan	Earthquake, registering 8.9 (Great) on the Richter Scale
April 14th-16th	Oklahoma to North Carolina	Tornados, causing at least 162 deaths.
April 19th	Mexico	Over 400,000 acres destroyed by wild fires. Fires surrounded cities of Acuña, Arteaga, Muzquiz, and Ocampo.
May 22nd	Iceland	Volcanic eruption halted all air travel within 120 nautical miles of the eruption.
April-May	Mississippi	One of the most damaging floods in the past century. Disrupted up to 13% of US petroleum refinery output.
June 1st	Massachusetts	Tornados, killing 3 (in a non tornado-prone location)
June 4th	Chile	Volcanic eruption for the first time in 50 years
July 5th	Arizona	Dust Storm travels 100 miles causing widespread respiratory problems
July 7th	New Zealand	Earthquake, magnitude 7.8 (Major)

Table 1. Major disasters in 2011

Mission CRITICAL
Data center and emergency backup solutions

Continued from page 6

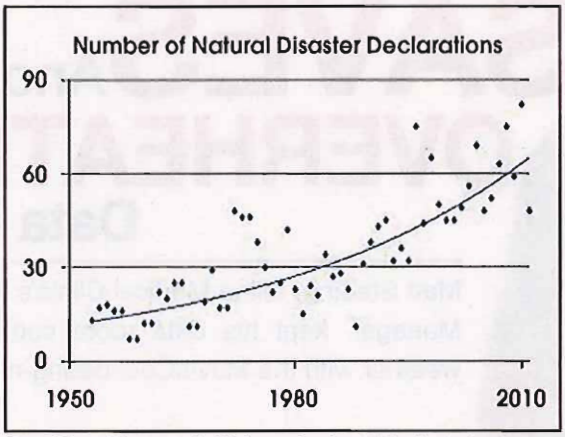

Figure 1. Natural disasters in the U.S. by year, based on FEMA table, "Declared Disasters by Year or State"

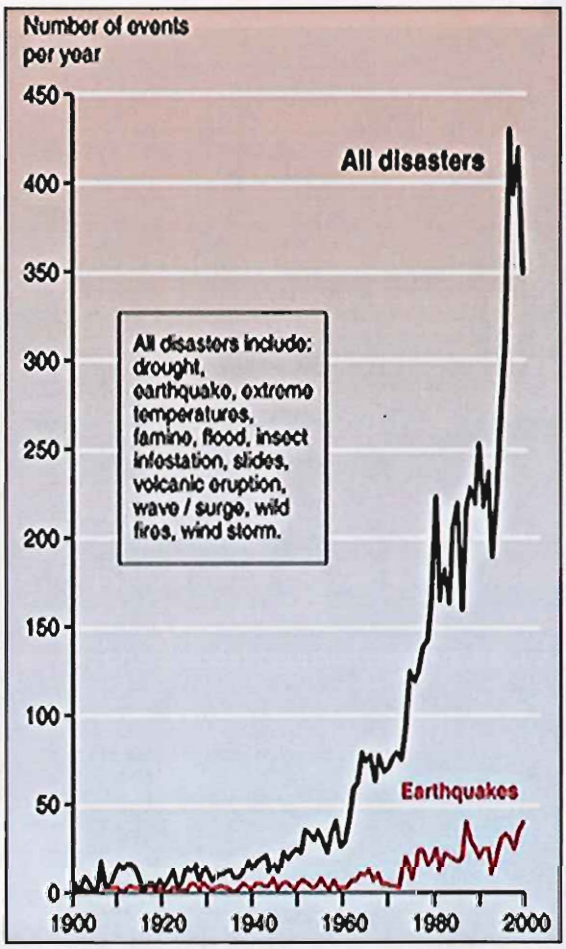

Figure 2. Global natural disasters by year
Source: Centre for Research on the Epidemiology of Disasters Emmanuelle Bournay, UNEP/GRID-Arendal http://maps.grida.no/go/graphic/trends-in-natural-disasters

eruptions, and earthquakes showed us that we never really know what we are up against.

Would we really say we are well protected against disaster were we to closely inspect the critical systems that we manage (including equipment, people, and process) and align them to the risk of downtime.

Facilities and IT professionals know how many near misses occur each year from a corporate/government perspective. Are these incidents increasing annually? Consider, for example, recent airline mishaps around the world stemming from human error. Pilots become complacent over time and lose focus while flying. This has resulted in several crashes as planes have veered off course and even collided on runways.

Furthermore, in the rail industry, an engineer was texting while operating a train in Los Angeles; the train subsequently crashed one minute after his final text message was sent. Even in fields requiring 100 percent success such as air/rail travel, human error is prevalent.

Now, let's assume your mission-critical facility is prepared because it has instituted the proper Tier rating based on its design intent and is reevaluated annually for internal and external risk factors. With all of the information breaches and the complex connectivity of diverse systems we operate, are you sure you are protected against someone hacking into your critical systems? These companies thought that they were (see table 2).

Some of the biggest companies in all areas of industry have fallen victim to hackers. Internet powerhouses, financial giants, defense contractors, e-commerce firms, etc., cannot keep criminals out of their systems. Criminals are upping the ante, and companies need to be able to match their bet. These breaches come at a crucial time in a society-wide movement towards "the cloud." Information is no longer stored on local machines; it is stored in data centers globally.

We must also consider security breaches from within. There have been instances where technicians servicing equipment brought in virus-infected laptops and/or USB flash drives. They then transferred files or used diagnostic tools on facility computers, thereby infecting them.

The Stuxnet virus (see Jan/Feb 2011, p. 30), for instance, was planted on an unsuspecting technician's USB drive from where it quickly spread throughout any computer system connected to the drive. The virus was capable of adjusting values in an industrial facility's PLCs and doing major damage.

If the mission-critical industry didn't have enough enemies as it were, we must also realize that budgetary constraints may be the cruelest villain of them all. On a facility scale, having maintenance budgets approved can be an exhausting battle. However, if the battle is chosen carefully, and funds are allocated wisely, an effective operations/maintenance/training strategy can be implemented with enormous benefit.

We've already discussed three risks faced by the mission-critical industry: natural disasters, malicious hackers, and economics. There are still two more risks: poor operations and faulty maintenance of critical systems and energy security.

Continued from page 8

Date	Company	Information Compromised
April 2nd	Epsilon	Email addresses and names of customers for Best Buy, Target, Citibank
April 23rd	Sony	Personal info (email, address, phone) Credit card information of Playstation Network and Qriosity subscribers
May 21st	Lockheed Martin	RSA breach allowed hackers to use VPN system to access LM's internal network
June 2nd	Google	Account information/passwords of government officials/journalists
July 12th	Booz Allen Hamilton	90,000 military personnel email addresses with crackable password hashes were copied. 4 GB of source code copied and erased from BAH server.

Table 2. Cyber security breaches in 2011

As you are already aware, human error accounts for greater than 60 percent of downtime in mission-critical facilities. While we can do our best to prevent operation and maintenance errors, it's almost impossible to completely eliminate them. According to the Energy Information Agency, the U.S. imports between 60 and 70 percent of the oil it uses for transportation and over 90 percent of the uranium used in the nation's nuclear power plants. As a result, a significant share our energy security lies in the hands of our suppliers. Adding up all these factors, and including our antiquated electric grid, makes it clear that we are now in the eye of the storm.

This storm may really be hiding a silver lining, an opportunity to make swift progress if we focus our attention in the right areas. These factors make designing and implementing a robust smart grid paramount to the safety and success of society today.

We cannot wait 30 years to make progress because we are at more risk every day. In addition, making immediate progress on the smart grid has a direct and sudden positive impact on creating jobs and improving our infrastructure. Doesn't this create an asset? Yes there is a significant upfront cost, but long term it is an annuity. This should be our political priority.

All the threats to society and the critical industry have raised the stakes, and we have to do whatever we can to stay ahead. The smart grid is an innovation we can and need to make in order to keep critical facilities resilient and facilitate economic recovery.

We need to take advantage of the capabilities we have; in this case, the smart grid can reverse the effects of the "steroids." Then we are only left with the "perfect storm," which we know isn't going to let up anytime soon. ■