The Washington Post
Date: Thursday, June 17, 2010
Location: WASHINGTON, DC
Circulation (DMA): 578,482 (8)
Type (Frequency): Newspaper (D)
Page: A8
Keyword: Yossi Sheffi

Reemphasizing value of duplicate safety systems

Flawed backup may be more dangerous than no plan, engineers say

BY DAVID A. FAHRENTHOLD

Airliners can lose one engine and keep flying. Nuclear power plants have two cooling systems, in case one fails. In an explosion, coal mines must allow miners two paths to escape.

So why didn't BP have a working Plan B?

From previous accidents, engineers have learned the value of duplicate, even triplicate, safety systems. The oil industry says it was following that maxim: By regulation, it installed giant machines called "blowout preventers" on drill pipes, with powerful bolts to close off a leaking pipe.

But at the Deepwater Horizon drilling rig, something went wrong. The backup plan failed.

Now, engineers say, the Gulf of Mexico spill has become another depressing test case in the value of redundancy. And, as the investigation unspools, it might be adding a corollary to the lesson: Having a Plan B that won't work might be more dangerous than having no plan at all.

"How can you go back and drill in deep water if you cannot tell the public that the probability of this happening again is almost zero?" said Paul Bommer, a lecturer in petroleum engineering at the University of Texas. "Whatever you thought you had [to prevent a disaster], you didn't have."

This week, former Environmental Protection Agency administrator William K. Reilly — chosen by President Obama as co-chairman of a national commission investigating the spill — said he wants to change the "safety culture" of the offshore drilling industry. He said that he wanted to start a safety organization similar to one that has focused on improvements at nuclear plants.

"Once that blowout occurred and got away from people, and the well couldn't be managed, it's difficult to imagine any" cleanup that could keep up, Reilly said in a telephone interview Wednesday.

The idea of safety through redundancy — engineers also call it "resilience" or "defense-in-depth" — is familiar to anyone who has walked past an airliner's cockpit. There are two seats in there, two pilots.

Other examples abound: The space shuttle has two ways of lowering its landing gear. Nuclear plants have several layers of containment between their cores and the outside world. Some cars with electronic acceleration have two systems for measuring how hard the driver pushes on the pedal: If they conflict, the car is supposed to stop accelerating.

Over the weekend, redundancy saved the historic battleship USS Texas, a tourist attraction outside Houston. A pump burned out, water leaked in and a backup pump system helped stop the 96-year-old ship from sinking.

"If you have a fire, you don't want to — at that point — start buying firetrucks and training people," said Yossi Sheffi, the director of MIT's Engineering Systems Division. Much of the time fire trucks and firefighters sit waiting, but he said that's the cost of being prepared.

For more than 25 years, the U.S. government has required offshore oil rigs to install a blowout preventer — a machine designed to be redundant within itself. The devices are required to include several "rams" that can be activated to close off sections of the pipe if oil or gas were to come up the hole suddenly.

In the worst-case scenario, a powerful "shear ram" would cut through the pipe completely. On the Deepwater Horizon, there were three separate ways to activate the device, including a "deadman" switch that would work if other systems failed. None apparantly worked.

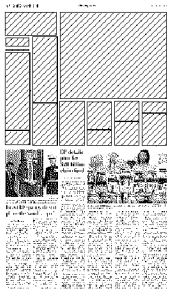
"This is it," said Erik Milito, of the American Petroleum Institute, an industry group. "The [blowout preventer] stack is the emergency response capability in the event of a blowout."

BP's Houston office did not respond to a message left seeking comment Wednesday.

In testimony prepared for a congressional hearing Thursday, BP chief executive Tony Hayward wrote: "Based on what happened on April 20, we now know we need better safety technology. We in the industry have long relied on the blowout preventer as the principal piece of safety equipment. Yet, on this occasion it apparently failed, with disastrous consequences."

Reilly's investigation must determine: Did the blowout preventer's failure result from something particular to this well? Or is this blast a sign that what looked like a redundant system actually wasn't and that a single event made all of its parts fail at once?

Since the spill began, congressional investigators have raised questions about problems with the Deepwater Horizon blowout



The Washington Post

Date: Thursday, June 17, 2010
Location: WASHINGTON, DC
Circulation (DMA): 578,482 (8)
Type (Frequency): Newspaper (D)
Page: A8
Keyword: Yossi Sheffi

preventer. The exact problems, of course, won't be known until the well is finally capped and the device raised from the gulf floor.

But 2004 documents show that the device had been modified at BP's request, so that one of the rams was replaced with a "test ram," which would be useless in an emergency. "The Conversion will reduce the built-in redundancy," a Transocean official wrote at the time. Also, an initial investigation after the blast seemed to show hydraulic fluid leaking out of the device — although a Transocean official later disputed that.

With those kinds of problems, "you end up with a hemophiliac system" in which one failure is catastrophic, said Robert Bea, an engineering professor at the University of California at Berkeley. "And nature has no tolerance for that sort of thing."

A spokesman for Transocean responded: "Until the investigations determine the cause of the catastrophic failure of the well and the subsequent effects that failure had on the BOP, it's difficult to render any judgments on the number of redundant systems that should be required in a subsea stack. As it was, the Deepwater Horizon BOP stack met and exceeded all such requirements."

If the investigation reveals a weakness in blowout preventers more generally, the oil industry might have to find a backup for its backup. In a May 19 hearing of the House transportation committee, Rep. Jason Altmire (D-Pa.) asked BP America President Lamar McKay to consider that possibility. "Is there any technology that exists that you know of that could have prevented this from happening?" Altmire asked.

"I don't know of a piece of technology that could have prevented it," McKay said.

fahrenthold@washpost.com

DAVE MARTIN/ASSOCIATED PRESS

BP said it is using a second method to capture oil from the damaged well, pulling it from the blowout preventer to this Q4000 rig.