Data center EPO vulnerability fixed in 2011 National Electrical Code

By Matt Stansberry, Executive Editor

05 Nov 2010 | SearchDataCenter.com

After years of wrangling with the National Fire Protection Association (NFPA) over the data center emergency power off (EPO) button, industry leaders have finally convinced the organization to modify its code to help companies avoid data center downtime.

The EPO, often a big, red pushbutton located near the data center exit, is designed to let firefighters shut down power quickly during a fire in the data center. Unfortunately, people push the EPO button accidentally or as an act of sabotage, causing what Uptime Institute founder Ken Brill has called "a corporate heart attack."

A group of industry leaders from AFCOM and Uptime started working together on this project in 2007, finding contacts within the NFPA, researching the history of the EPO, and traveling around the country to build consensus and educate NFPA code panel members.

David Boston, data center consultant and former manager of the Site Uptime Network, said during the June 2010 meeting of NFPA members, a proposal to modify NFPA 70 Article 645-10 cleared its last opportunity for objections. It is now on its way to the Standards Board for final review and will be included in the 2011 National Electrical Code, due to be published late this year and issued in January 2011.

Boston said this will allow data center owners to construct or retrofit their facilities without needing to place an EPO switch at each principal exit. Instead:

"Owners will have the ability to negotiate a preferred EPO location within their facility with the local Authority Having Jurisdiction (AHJ), thereby reducing the risk of accidental or malicious power interruption. Owners who meet more stringent criteria will have the option, if the AHJ concurs, to construct their facility with no EPO (an alternate means of disconnecting power in the event of fire will be required)."

Data center EPO horror stories abound

Tom Roberts, an AFCOM board member and a data center facilities manager for Trinity Information Services, a healthcare company in Farmington Hills, Mich., has seen *two* data center outages due to an EPO misfire.

Roberts rolled out a brand new data center in the spring of 2003. Trinity had dedicated the building and was starting to bring clinical applications online when the facility took an EPO hit on Easter Sunday.

The event resulted in mass confusion and illustrated how vulnerable the systems were from a single source of interruption, Roberts said. And these buttons were scattered throughout the building.

That experience lit a fire under Roberts, who decided to take the issue to his local fire marshal, who agreed that the uptime of the healthcare provider's data center was critical. The local fire authority allowed Roberts to leave the EPO system in bypass (meaning it wouldn't shut down the systems unless the bypass was engaged by facilities staff). But due to a mistake in the building plan schematics, there was a loop around the EPO circuit that Roberts wasn't aware of, so the bypass didn't work. Trinity took another EPO hit in 2008.

At that point, Roberts vowed not to retire until this problem was addressed. "Now it's fixed, I can't retire because of the economy!" Roberts said.

Where did the data center EPO requirement come from?

Data center pros have battled the EPO requirement for years. Some huge companies threw their weight around with the NFPA, but to no avail. So how did this effort succeed?

Richard Schlosser, President at Baltimore-based data center design firm TiePoint Engineering, said getting the code changed depended on getting buy-in from the fire protection community, and understanding where the regulation came from in the first place.

Schlosser was on the committee to pursue the code change, and researched the history of the data center EPO. He spent a week in a library in Braintree, Mass., researching codes and figuring out when it first showed up in the National Electric Code, and traced it back to a huge data center fire in the Pentagon in1959.

According to the Arlington Fire Journal:

"The flames erupted in a computer room operated by an Air Force statistical agency and burned for more than five hours -- fueled by magnetic tape. There were no sprinklers. The blaze scorched 4,000 square feet and caused $30 million damage to the massive building and the computer equipment."

Schlosser said Congress then went to the NFPA and asked the group to write rules protecting data centers in the event of fires. "They came up with a whole new set of rules, including a kill switch for the data center console," Schlosser said.

Scaling back safety requirements for fire service first responders wasn't easy, Schlosser added. For the data center industry, putting a big red button next to the door that anybody can punch isn't convenient. But fire service professionals consider the EPO a life-saving measure.

"We've created the environment [so] that the fire fighters think they needed a kill switch at the door. It was a big deal for them to relinquish that control," Schlosser said. "They feel like it's a big step backwards from a life safety perspective."

Instead of fighting this uphill battle, the committee decided to try to befriend the authorities and provide some alternatives.

Schlosser said one option is to put a supervisor on duty 24 hours a day. This person would be trained and qualified to shut the place down and would be continuously available to meet fire responders when they show up and go through an approved procedure before entering the facility with axes and hoses. The other alternative is to move the EPO away from the exit doors into an area that is under control of management. “Firefighters can go into a locked room and shut down the data center from there,” Schlosser said. “It’s just like an elevator closet or electrical room. It’s not accessible to the main public in the building, but authorized people have access.”

Dealing with your local fire authority on data center EPO issues

While the new National Electrical Code is headed to the printer right now, and the change will be on the books for 2011, it could take one to three years for local jurisdictions to adopt the new code. For most data centers this will mean it’ll take effect in the 2013-2014 time frame.

What can you do to speed up the process? Roberts recommends asking your fire marshal, or local Authority Having Jurisdiction (AHJ) in fire-speak, if they will adopt the 2011 code early.

“If you’re a data center facility person, you need to get intimate with these guys,” Roberts said. “You need to know what their expectations are. Those guys have tough jobs, inspecting multistory buildings, old factories, but if I can help them learn the small area I know about, it’s better to both of us. If I can get close to those guys it helps.”

What did you think of this feature? Write to SearchDataCenter.com's Matt Stansberry about your data center concerns at mstansberry@techtarget.com.