Digital Power

By Peter M. Curtis

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

The Next Decade: Expectations for the Unexpected

An unpredictable decade follows a turbulent one

As I look back on the last decade, I think it would be a major understatement to call it interesting. We approached it with the trepidation brought on by Y2K uncertainties, which proved to be nothing compared to the bursting of the dot-com bubble. Things got worse on 9/11, and the 2003 Northeast Blackout brought on heightened concern over business continuity/resiliency. Concerns over energy and global warming continued as the decade drew to a close even while collateralized debt obligations came home to roost and nearly brought the U.S. financial system to its knees.

These events are perfect examples of why the U.S. needs a robust infrastructure to keep its economy functioning no matter what happens. Considering all the changes we have collectively experienced during the last 10 years, I'm not certain what to expect going forward, but I am certain we will see more furious change, even greater than the previous decade.

In the twilight of the "The Digital Decade," we are all aware that the mission-critical industry has grown and transitioned at a tumultuous and rapid pace. Driving this intensity are the business requirements to process more, save more, and store more—all with reduced greenhouse gas production—while each day we manufacture, process, and store amounts of information equal to eight times the amount of information housed in all U.S. libraries combined.

When we first began the decade, acronyms and terms such as LEED, PUE, DCiE, virtualization, GHG, REC, mobile technology environments, and containerized systems, etc., either did not exist or did not affect this industry. Green practices in North America were mostly an afterthought in the data center environment until around mid-2006.

As we transition into the next decade much more attention will be focused on the smart grid, cloud computing, utility computing, and we must address ever growing threats such as cyberattacks, electronic warfare, and electromagnetic pulse weapons with a sense of urgency.

This past decade has seen a tremendous growth in Internet applications, and our dependence on them continues to increase, especially with all the new mobile devices and applications entering the market. For example, in 2003 online holiday sales totaled about $18.1 billion. Only six years later retailers saw close to $50 billion in online sales in the 2009 holiday season, and many retailers are now also utilizing social networking websites to promote sales and distribute coupons.

Behind the scenes, data centers requiring 20 to 50 MW of power now process anything from orders to inventory; the requirements in this decade have definitely changed. We now expect and have become dependent on technology to work continuously, so much so that when it's not available everything changes, just as it did in during the 2003 Northeast Blackout and to a lesser extent with failures of RIM's Blackberry network. If one of these large data centers were to go down during a period of high demand, the monetary losses would be absolutely devastating to the customer and the company.

As an industry, we must continue to update and refine the requirements that will improve our critical infrastructure and articulate the importance of security in all aspects—whether we are securing our sensitive physical spaces, our energy grid, our BMS systems, or our IT assets. Cyberattacks are becoming more frequent, targeted, and sophisticated. The Department of Homeland Security, which is responsible for protecting civilian computer systems, suffered 850 cyberattacks in the two years from 2005 to 2007. Clearly security is a key component in development of the smart grid, utility computing, and cloud computing in assuring these emerging technologies are protected from a cyberattack and exposure to a third party with malicious intent.

So as we enter the next decade and start taking inventory, perhaps a place to begin is with your BMS System; does your building management system have a firewall? What protection do you have if someone were to hack into it? Just think about what it controls… this is just the beginning. We need to be prepared for anything, because whatever we can't imagine today is what we are going to have to deal with tomorrow, and we can't afford to be caught with our heads in the sand. ■