VEC Buys Morris Automation

VEC Supply (Virginia Electronic Components), Charlottesville, Va., a distributor of electronic components and services the focuses on the VDV, industrial automation, security, access control and OEM markets, acquired industrial automation specialist Morris Automation Group, Roanoke, Va. Morris Automation will operate as a standalone division of VEC and will continue to support the industrial automation marketplace.

In a press release announcing the acquisition, Frank Stalzer, VEC's president, said, "We believe this is an excellent add-on to the VEC business bringing us some new world-class product lines and a strong customer base of industrial accounts. Our goal is to continue to build our business organically and through acquisitions and this latest move brings our number of branch locations to four."

VEC maintains stocking sales branches in Lynchburg and Roanoke, Va., as well as Raleigh, N.C. In addition, VEC maintains an online distribution business operating under the banner DirectDatacom. The company's line card has some familiar names from the mainstream electrical industry, including Alpha Wire, Arlington Industries, Belden, Brady, Bussmann, Cooper Wiring Devices, Erico and WireXpress.

Stalzer told *EM* in an e-mail that with the Morris acquisition comes some new product lines, including Idec relays, Micron transformers, Optex sensors, Fuji switches and circuit breakers and Luxor tower lights. Both companies are ABB distributors, and Stalzer says the acquisition makes VEC a "much bigger play with the ABB line."

Commerce Affirms Tariffs on China Solar Cells

The U.S. Department of Commerce (DoC) announced its affirmative final determinations in the anti-dumping and countervailing duty investigations of crystalline silicon photovoltaic cells imported from the People's Republic of China. DoC determined that Chinese producers and exporters have sold solar cells in the United States at dumping margins ranging from 18.32% to 249.96%. DoC also determined Chinese producers and exporters have received countervailable subsidies of 14.78% to 15.97%. The department said in a factsheet released Oct. 10 that it will instruct U.S. Customs and Border Protection to collect cash deposits and bonds equal to the dumping margins, less a subsidy rate. Further enforcement will depend on a final determination from the International Trade Commission, due by Nov. 23.

EW NEWS ANALYSIS

Schneider's Telvent Responds to Network Attack

News last month of a hacker's attack on the networks of infrastructure control system provider Telvent Canada Ltd., a unit of Schneider Electric, threw a spotlight on existing concerns about the security of critical infrastructure.

Telvent discovered an intrusion on its network affecting systems in Canada, the United States and Spain. The breach affected customer project files related to Telvent's OASyS DNA supervisory control and data acquisition (SCADA) software. Some of those files were reportedly stolen and malicious software was installed on the company's network.

Telvent's SCADA systems are used by electric, oil and gas, water and transportation providers for real-time control of their operations. The concern that intruders could disrupt utility operations by infiltrating system providers who have "back-door" access to customer systems is a source of ongoing and urgent behind-the-scenes work by utilities and their system providers. The companies involved seldom publicize their efforts in this area, which escalated in 2010 after the Stuxnet worm attack on Iranian nuclear facilities demonstrated that it was possible to gain control of mission-critical SCADA systems.

Telvent and Schneider have declined to speak in detail about the hack attack. Martin Hanna, vice president of press relations for Schneider's North American operations based in Palatine, Ill., provided *Electrical Wholesaling* with the following statement and declined to elaborate:

"Telvent is aware of a security breach of its corporate network that has affected some customer files. Customers have been informed and are taking recommended actions, with the support of Telvent teams. Telvent is actively working with law enforcement, security specialists and its affected customers to ensure the breach has been contained."

Hanna did confirm that letters were sent to Telvent customers starting on Sept. 10 when it learned of a breach of its internal firewall and security systems. The letters said Telvent had indefinitely shut down its access to customer systems even though it had found no evidence that the intruder had acquired any information that would enable them to gain access to a customer system.