86e Developing a Manufacturing Control System Cybersecurity Program: Case Study and Developing Standards

Dave Mills

Several factors have led to growing risks associated with the use of manufacturing control systems. These factors include threats that are growing either in frequency (viruses and worms) or seriousness (terrorism), the widespread use of technologies that were not designed with security as a high-priority attribute, growing levels of connectivity between manufacturing control systems and higher-level business systems to achieve greater levels of productivity, and work processes that ignored the risk because historically these manufacturing control systems were not network-connected. In the aftermath of the 9/11 attacks corporations have begun to reexamine these risks and establish Cybersecurity programs to deal with them. The experience of Procter & Gamble provides a case study in how this process has evolved in one corporation and also provides an introduction to the international standards that are being developed in this area.

These Cybersecurity programs are based on the risk management models that have been developed for process safety, personnel safety and environmental risk management but incorporate links into the IT organizations that typically own the Cybersecurity risks to corporate networks. These programs also involve linkages with physical security and business continuity planning. The scope of these programs includes technical issues such as network architecture, access control, use of anti-virus products and patch management as well as work process issues such as leadership, communication, coordination, results tracking and disaster recovery planning with the focus being to cost-effectively reduce risk to the organization.