Com exCu: Industrial wireless

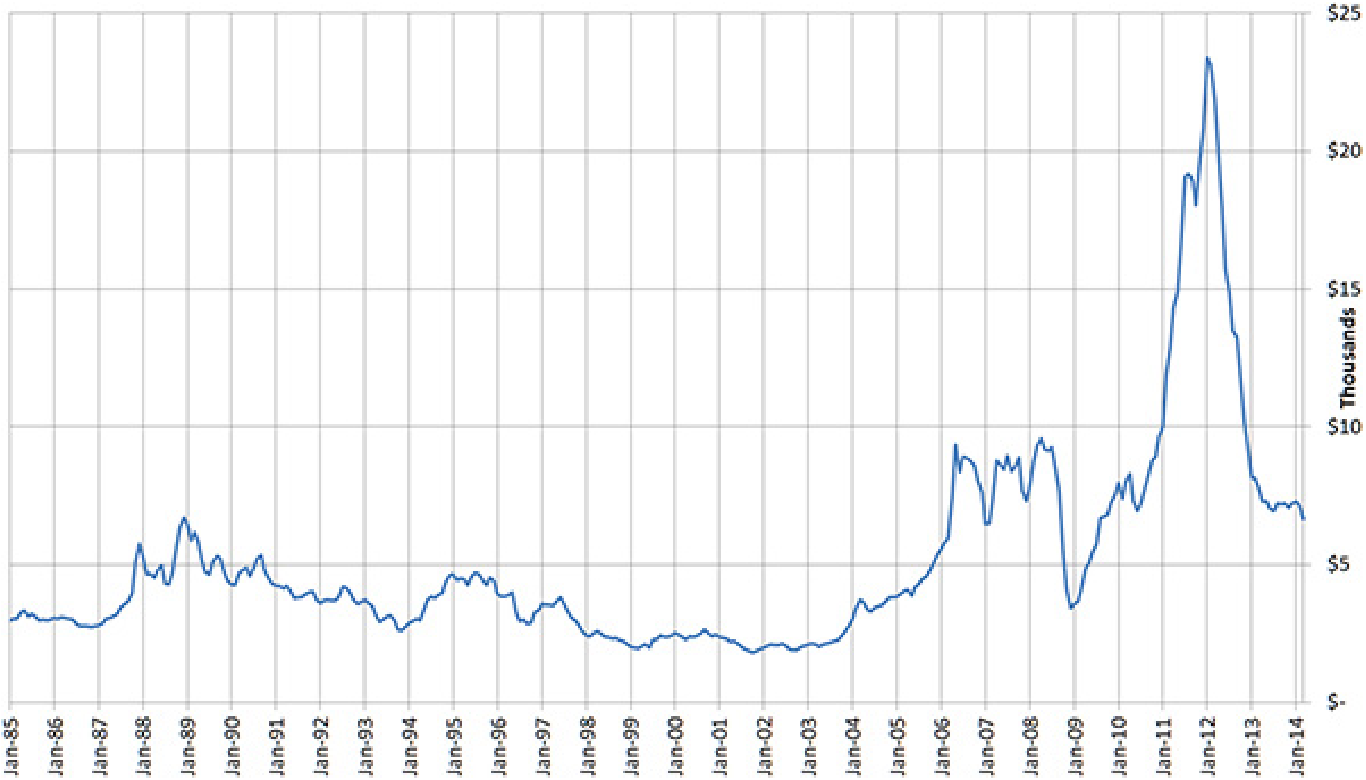
Joshua Israelsohn, Director, JAS Technical Media

Like general-purpose computational resources in commercial enterprises, factory automation systems have evolved from highly centralized structures with fixed peripheral connections to flexible models with distributed intelligence and networked I/O nodes. In the factory environment, networking and distributed intelligence increased resource availability and reduced scaling costs. It also eliminated a degree of systemic brittleness, allowing factory owners to reallocate production resources more quickly and to take better advantage of equipment suppliers’ process expertise.

Such system flexibility facilitated an increase of sensing and actuation nodes, both in number and type, to support improved process quality, yield, and safety for equipment, WIP (work in process) inventory, and human operators on the factory floor. Sensing examples include common measures of temperature, pressure, mass, and flow rate that require low to moderate data rates but also include greater use of motion control and image captures that demand high-bandwidth communication links.

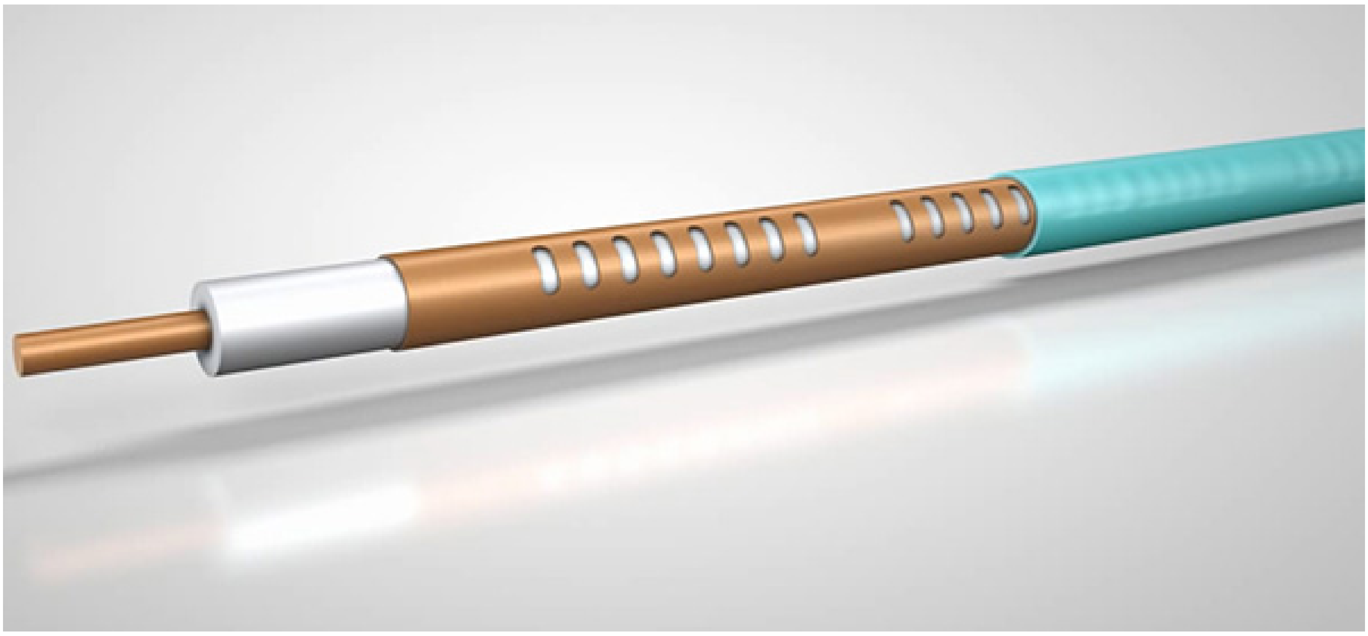
Process-control equipment manufacturers have also shifted from proprietary to standards-basedcommunication methods. Although, over the years, the industry has developed several communication protocols to meet the specific demands of real-time applications, the trend has been toward more general-purpose technologies. This is possible for two reasons: GP communication speeds have greatly increased and message latencies have decreased in the time since process control systems adopted networked architectures. The distributed intelligence model also keeps the control elements for real-time control loops close to the measurement-and-control nodes and less time-critical data flows between the controllers and the process-management system.

Maintenance and reconfiguration costs remain high, however, partly due to wiring; the installation and repair of which is labor intensive. This has been particularly true, as copper commodity prices have exhibited uncharacteristically high volatility in recent years (**Figure 1**). The switch to industrial wireless systems, however, has not been a simple swap of media and physical-layer devices.



The choice of radio-link technology must accommodate a node's or node cluster's operating requirements. For example, low data rate, low duty cycle nodes that must operate on a minimum power budget can use low energy Zigbee links over short distances. In some cases, such and temperature or machine-health monitors, an energy harvester can power a sensor, digitizer, and radio thereby eliminating the copper connections for power as well as for data.

In electromagnetically noisy environments, radiating cable can form a distributed antenna for a robust radio link to moving equipment. For example, Siemens' RCoax radiates radio waves through small holes in its outer conductor forming a spatially-limited link (**Figure 2**). This arrangement minimizes the extent to which the transmitted energy couples to other wireless equipment while providing a radio link that is robust in the presence of high RFI fields. RCoax is compatible with Profinet for applications such as cranes, storage and retrieval vehicles, or monorail-mounted trolleys.



For high data-rate applications, such as imaging, several companies have adopted wireless Ethernet radios such as those conforming to IEEE 802.11n. These can provide data bandwidths to 450 Mbps and, with careful channel allocations, operate with a low degree of mutual interference with other nearby radios.

The ability to access factory data on an associated enterprise network allows real-time monitoring of inventory and WIP. It also allows companies to merge their factory inventory-control system with their supply-chain management.

However, as more factory equipment is accessible on line through IP communication channels and enterprise networks extend outside a single facility, network and equipment security is an increasing concern. In systems that make use of proprietary formulae or processes, even the security and authentication of individual process tools are issues that the system design may need to resolve.