wireless or wired systems — Siemens has the right technology for every situation.

Reliable communication systems that extend from the factory floor to plant offices — to production managers, suppliers, and distributors more rapidly and flexibly.

That’s the vision of the seamless factory,” says Röhrl, referring to merchandise management (see pp. 13, 16). Production floors, development, production control, and offices are thus set to converge globally.

Röhrl, head of Product Management at Industrial Communication at Siemens Automation and Drives (A&D) in Nuremberg, Germany, is having an impact on everyone in the product process — from product designers to production managers, suppliers, and distributors, all of whom need to access relevant product data more quickly than ever before.

“We work on our product databases six days a week, 24 hours a day,” says Röhrl. “This is why we need to be able to access product data across all local interfaces and in real-time.”

“IWLAN technology is very complex because factories contain a lot of equipment that can interfere with signals. There are metal machines, devices that emit electromagnetic waves, and areas with very high temperatures and vibrations. Uninterrupted connections can be ensured by using special materials for receiving housings and secure installations for circuit boards from Siemens’ Scalance W product family. In addition, encryption and access control systems do their part to protect against external computer attacks. At the 2007 Hannover Fair, Siemens presented a new wireless emergency cut-off security feature. “Our IWLAN system makes it possible for the first time to not only securely monitor a facility but also securely operate it,” says Kuk. “Emergency shut-down circuit breakers are usually triggered via separate cables. With Siemens’ IWLAN system, however, the emergency signal is securely transmitted within fractions of a second in the reserved data transfer packet.”

Thanks to the increasing performance capability of a broad range of components, industrial communication systems are becoming ever more seamless — all the way down to the level of sensors and actuators. Sensors register information across all local interfaces. “This method will be Ethernet,” says Röhrl. “Ethernet is nothing new. It’s been used for more than 30 years to link office computers, while Industrial Ethernet has been networking production control systems for over 20 years. Now, however, Ethernet is set to take control of individual machines in factories.

Data that’s Always There. Yet significant challenges remain to be overcome. "The big issue is real-time data transmission," says Ewald Kuk, head of Product Management at Industrial Communication. "In office Ethernet systems, if a data packet has to wait a couple of seconds because the information highway is occupied, no one will notice." But that can’t be tolerated if data is transmitted to production machines, the control processes for which often occur in the space of milliseconds or even microseconds. "Imagine a printing machine with several rollers," says Kuk. “If just one roller fails to operate completely in sync with the others, you can throw away the result. That’s why we’ve developed an industrial Ethernet system that always keeps a high-priority lane open for time-critical data." (See Pictures of the Future, Fall 2005, p. 34). Because Industrial Ethernet is based on the office network standard, it has no problems with interface linkage.

But not all production areas can be connected via cables, which is why wireless solutions should be employed in difficult-to-reach areas, not to mention when it comes to driverless transport systems and rotating components. Audi, for example, uses IWLAN (Industrial Wireless Local Area Network) in the production of its R8 sports car: Here, the vehicle body is mounted on a device that can rotate 360 degrees, enabling bolting robots to reach every corner. Because IWLAN is based on the WLAN standard, it can easily be integrated into existing networks and Ethernet systems, whereby the wireless connection presents a challenge in addition to the real-time issue in that it needs to be reliable at all times. “If your cell phone drops a call, you can redial, but an interruption to the radio signal in a factory will result in expensive losses after just a few minutes,” Kuk explains. IWLAN therefore uses redundant antennas, reserved data transfer packets, a time-monitored signal transmission system and a roaming function to ensure continuous connections. “Thanks to its patented innovations, Siemens has a lead of at least one-and-a-half years on the competition when it comes to reliable wireless data communication,” says Kuk.

Intelligent algorithms and growing computing power on chips open up completely new application possibilities for these sensor networks, as they are now capable of self-organization. Individual sensors can start themselves up, recognize neighboring sensors, and communicate with them, meaning that if one sensor fails, another can pass on the information that would otherwise have been lost.

Such systems are known as mesh networks because they link sensors like a lattice, which is what distinguishes them from previous star-shaped architectures in which each node could only communicate with neighboring devices. "Self-organization makes wireless systems more flexible and robust, and also significantly lowers planning and operating costs," says Dr. Rainer Sauerwein, a self-organization researcher at Siemens Corporate Technology. "This is especially helpful when the network topology cannot be planned in advance." This would be the case, for example, if a truck driving between two oil tanks at a refinery had its wireless connection interrupted. Sauerwein and his colleagues are developing new wireless technologies to ensure that sensors can be utilized as flexibly as possible in production. But such systems need to be immune to disturbances from other radio fields in the factory environment. “The most interesting standard here at the moment is ultra-wide band, or UWB,” Sauerwein says. “Unlike nar-
Many production plants are linked to the Internet and utilize standard software, which makes them a potential target for hackers. Siemens is making these systems more secure.

Things are running smoothly in the plant. A robot moves car bodies to the next work station, where assembly workers are waiting, and the IT officer has informed the production manager that the robot control system is completely secured against hacker attacks. “We’ve got effective passwords, secure encryption, and an impenetrable firewall,” he announces. As it turns out, he’s wrong. A hacker has just entered the system by using a Google search to find the production control home page. He tries out a couple of simple passwords, but to no avail. Then he launches what’s known as an SQL injection. Instead of using a password, he copies into the entry a short piece of program code and manipulates the database, which contains security-related information. He is thus able to open the lock without using a key, as it were. Now things begin to move quickly. The hacker has found his way into the production line control system. He issues a command to stop a robot, which then proceeds to open its gripping arm, causing a heavy body shell component to fall directly on top of a worker.

Murmuring can now be heard in the auditory as the lights go on, and the 300 people at an in-house Siemens fair in February 2007 are completely shocked at how easily Dr. Konstan-

Tin Knorl has been able to shut down a factory production system. They’re relieved, though, that the robot is only a prop and the “injured” worker merely a plastic figure. “Still, it gets their attention,” says Knorl, who uses this demonstration to make his colleagues more se-

curity conscious. Knorl is one of approximately 70 people at Siemens Corporate Technology (CT) in Munich who provide advice on security issues to various Siemens units. Those who work in this area need not be former hackers or ex-cops; they only need to be in possession of a college degree “and have a well-developed sense of morality,” according to Dr. Johann Fichtner, head of the CER

(Technology) in Munich who provide advice on security issues to various Siemens units. Those who work in this area need not be former hackers or ex-cops; they only need to be in possession of a college degree “and have a well-developed sense of morality,” according to Dr. Johann Fichtner, head of the CERT (Siemens’ Computer Emergency Response Team) Center.

The goal of such CT demonstrations is to raise security awareness among people who work with IT systems, and support secure plan-

ning measures for future Siemens products. Se-

curity requirements have risen dramatically in recent years — and not just at Siemens. Whereas control systems for production lines and power plants used to be completely isolated from the outside world and emply specialized software, they now often run on standard software like Windows and utilize off-

line databases. More importantly, how-

ever, they are increasingly being linked to the Internet for remote maintenance and other services. The risk of external attack is therefore greater than ever before. In addition, tax depre-

ciation periods for factories, power plants, and hospitals are now longer, which means IT sys-

tems are not replaced every three-to-five years as is the case with office PCs. As a result, the latest security updates are not always available. Robust IT Systems for Power Distribution. Just how important cyber-security can be is demon-

strated by a system failure that occurred at the Davis-Besse nuclear power plant in Ohio on January 25, 2003, when the Sliermann worm entered the facility’s IT network through the In-

ternet and shut down parts of it for nearly five hours. Fortunately, nothing happened because the plant happened to be shut off for repairs at the time. Whoever launched the attack took advantage of a security hole in a database that Microsoft had actually offered an update for six months earlier. But unfortunately, the software programmers in charge of security at the plant didn’t know about that.

To prevent such an event from happening with software from Siemens, the company’s Corporate Technology department, which Fichte-

ner’s team is a part of, offers sophisticated so-

lutions for all Siemens operations. One such system is being used at Siemens Power Trans-

mission and Distribution’s (PTD) Energy Auto-

mation unit in Nuremberg, where Bernd Nart-

mann serves as a product manager whose

responsibilities include security issues. Two years ago, Nartmann asked CERT to look for weak spots in the product portfolio through which hackers might enter the system. This ex-

amination was necessitated by the fact that the unit’s customers (in most cases major power supply companies) were increasingly utilizing public communication networks to collect data and issue switching commands. Some compo-

ents, such as switching and fuse modules for high-voltage facilities, are more than 30 years old, but “back then nobody could have known

Machines that Talk to Each Other

Machine-to-Machine Communication (M2M) is the automated exchange of data between machines. While M2M enables the transmission of data over great distances via mobile radio, it cannot provide for the real-time transfer needed in production. That’s why long-distance M2M networks are best employed in areas where WLAN or industrial Ethernet are not economically viable options and there are no time-critical applications to consider — such as, for instance, monitoring giant pipelines in open country. M2M technology from Siemens can be used for systems such as beverage machines that notify a central warehouse when they need to be refilled, or electric meters that radio readings to utility companies. Freight forwarders can also utilize M2M to have truck data relayed to headquarters...