

# Factory Monitoring and Control Using the Internet

Alfred C. Weaver  
Department of Computer Science  
University of Virginia  
151 Engineer's Way  
Charlottesville, VA 22904  
weaver@virginia.edu

**Abstract** – In this one-hour tutorial we explore the premise that the Internet and the World Wide Web, when combined with the software tools developed to support electronic commerce, are the enabling factors for achieving remote factory monitoring and control (and, ultimately, industrial control in general). We look briefly at the issues of system architecture; web protocols and services; wired and wireless access; Java programming; Jini lookup services; multimedia; multicast; privacy and security; reliability; factory monitoring; instrument control; and the research challenges for fast, closed-loop, real-time control.

## I. REUSABLE INTERNET RESOURCES

Our premise is that industrial monitoring and control are enabled by the hardware and software already developed to support electronic commerce over the Internet and World Wide Web. We show by example why this is so.

**Wireless Internet Access.** WAP (Wireless Applications Protocol) is an emerging standard that will permit wireless telephones and PDAs to interact with Internet appliances ranging from parking meters and drink dispensers to household devices, automobiles, and factory equipment. WAP-enabled devices are just now appearing in the marketplace. Bluetooth is an emerging standard for short-range (10 m) wireless communications. Bluetooth implements both infrared and RF communication and will provide the physical communications channel among communicating devices. IEEE 802.11b is the new standard for wireless Ethernet; it operates at 11 Mbps and is especially useful for connecting mobile laptops to a resident computing infrastructure using a low-cost PCMCIA adapter card.

**Java Programming.** Java is a programming language designed from the outset to be portable, thereby minimizing the effort required to port an application from one computer to another. Java borrows heavily from the popular C and C++ languages, and thus is reasonably easy to learn. Java is portable because the language produces an intermediate code (bytecodes) that is then interpreted at run-time, and the run-time interpreter is provided transparently in all modern web browsers.

**Jini.** Jini is a set of specifications that enables services to discover one another. Jini is not about hardware or devices, it is about services. An example use would be bringing a laptop into a room and having it find – without human intervention – what print and display services are available, attach to them, and configure itself for them.

**Multimedia.** The successful deployment of a modern industrial automation system today requires much more than the exchange of process data needed for monitoring and

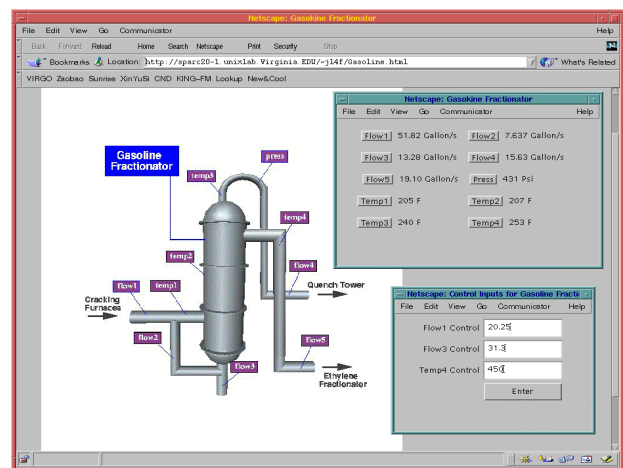
control. As network bandwidth increases, audio and video are now used for a variety of purposes ranging from live monitoring of processes to security systems to broadcast of educational materials.

**Multicast.** We see many new applications in which there are multiple recipients for a single data stream. In the context of traditional entertainment, the large viewing audience for a popular movie or a Super Bowl broadcast exemplifies this; in the industrial context, the analogy would be multiple simultaneous viewers of an assembly process, or multiple participants in a videoconference, or multiple viewers of an industrial training video.

**Information Security.** No company would use the Internet to transmit its proprietary information if it thought that its data could be copied, diverted, or altered enroute. A partial solution to data security is encryption. Symmetric key encryption and public key encryption are two methods that can be used to protect data and to authenticate the user of that data.

**Reliability.** As has been demonstrated repeatedly, hackers can bring down a site that is not properly protected. Firewalls, proxy servers, load balancers, and other techniques can be used to avoid a distributed denial of service attack.

**Virtual Factory.** We show how a simulated petrochemical plant can be instrumented such that its pressures, temperatures, and flow rates can be monitored using a web browser by any authorized viewer.



A Java Applet Implements the Virtual Factory

**Control.** We close with a discussion of the challenges involved in achieving fast, real-time, closed-loop control over the public Internet.