# Appendix 1

## Networked Microsensors and the End of the World As We Know It

*Shepherd, D.*

Strategic Analysis Inc., Arlington, VA, USA; *This paper appears in:* **Technology and Society Magazine, IEEE**

Publication Date: Spring 2003

On page(s): 16–22

Volume: 22, Issue: 1

ISSN: 0278-0097

INSPEC Accession Number: 7556263

## Abstract

Microsensors promise to bring people into closer contact with computers and, in the process, change society significantly. The author examines the impact of sensors on four areas: industrial manufacturing, military operations, personal health, and individual freedoms.

## Index Terms

microsensors social aspects of automation technological forecasting individual freedoms industrial manufacturing microsensors military operations networked sensors

# Appendix 2

Microsensors promise to bring people into closer contact with computers and, in the process, change society significantly (and not necessarily for the better). Sensors and actuators link the world of events, tangible things, and organic creatures with the electronic world of computers, processors, and storage devices. Sensors accomplish this by integrating analog sensing with digital processing into a more efficient network where electronic fingers and tendrils pervade our lives and send signals to powerful databases and processors. Collaboration among the sensors – each of which will be a tiny computer (albeit comparatively low power and poor performance) – will enable real-time adaptation to environmental and user conditions and ensure that the whole becomes greater than the sum of the parts. Networked sensors will be remarkably responsive because of the quantity and quality (such as timeliness) of information provided to processors. The size of sensors and actuators will decrease to the point that actuators eventually will be small enough to course through individuals' bloodstreams and dispense medicine according to signals from similarly sized sensors. In some cases the sensors themselves will be organic elements of the body, sensing conditions and perhaps reporting to processors within the body or outside of it[1].

At this early stage of technological development, however, most people have not contemplated the ramifications of a society filled with sensors [2], [3]. One view of the future is provided by the founders of Ember Corporation, who envision a future when "every vine in a vineyard reports sunlight, temperature, and moisture every hour of the day, [when] every city street lamp monitors the passage of each bus" and relays information ahead to waiting passengers[2]. In other words, for the first time people will be able to monitor and control almost all aspects of their environment – including, potentially, other people. The social implications of this shift to integrated sensing and processing are enormous and varied, and probably are not entirely welcome to even the most enthusiastic technology proponent. Following are discussions examining the impact of sensors on four areas: industrial manufacturing, military operations, personal health, and individual freedoms [4].

## Industrial Applications

Sensors already play an important role in industry. For several decades sensors without many internal smarts have been placed on or in machines to monitor wear, heat, lubrication levels, or similar information. In more recent years, though, with the diminishing size of the sensors and increasing power of computers and networks, industry experts have realized the value that sensors can add to a manufacturing or monitoring effort. Sensors have become "smart," or imbued with the capability to read data faster, process and manipulate it in more ways, and transmit it to multiple destinations for display, storage, or further processing. And with the rise of the networked, intelligent factory, the use of sensors has blossomed. For example, the

"Buyer's Guide 2002," produced by *Sensors*, a trade publication in existence for 18 years, lists 116 physical properties sensed, 79 technologies used in making and employing sensors, and more than 1900 suppliers, manufacturers, and solutions providers. *Sensors* itself has almost 80 000 paid subscribers and, among many related sections, has a feature section titled, "Putting Sensors to Work," devoted to sensors' role in industry[3].

The Institute for Electrical and Electronics Engineers (IEEE) is facilitating the implementation of sensors in industry. Until a few years ago there was no standard method of connecting sensors to networks; manufacturers produced what clients needed, or as clients or applications demanded. This resulted in a hodgepodge of sensors, fieldbus hardware, and interface software – a technological tower of Babel. Industry experts realized that for sensors to gain acceptance, let alone widespread use, interfaces and connections would have to be standardized. As a result, the IEEE Instrumentation and Measurement Society and the National Institute for Standards and Technology (NIST) launched the P1451 Smart Transducer Interface Standard to standardize sensors for use in industry in a "plug-and-play" fashion. This is intended to unscramble the assortment of technologies and ideas about connecting sensors to processors and networks. The latest version of the standard, 1451.2, calls for an electronic data sheet in sensor modules to ensure proper data formatting, and a digital interface to enable processors and networks to access the data sheet and to set actuators [5]–[7]. IEEE is also sponsoring a working group around the emerging standard for personal area networks (PANs), 802.15. Personal area networks are defined to have a radius of 5 to 10 m, a relatively tiny range well suited to deployment of multiple microsensors that blanket an area and connect in a mesh topology to provide redundancy and eliminate single points of failure. Like the Bluetooth concept of short-range wireless devices to eliminate wiring and facilitate flexibility, 802.15 promises to usher in an era of multiple devices interconnected using short-range links.

**At this early stage of technological development, most people have not contemplated the ramifications of a society filled with sensors.**

This shift to more sensors, wired into factories and wireless in meshes, means that more goods can be produced in an automated fashion to exacting standards, thus increasing efficiency and decreasing waste. It also means that the goods produced by the factories can be instrumented to report machinery and product status in real time for use by the internal operations of the machine or equipment or for later use as conditions or users warrant. Similar sensors are currently used in automobiles to read pollution levels in the exhaust system as the engine runs, and to sense deceleration for use by airbag deployment triggers. In addition, sensors and actuators help to extend the life of plant equipment by enabling better diagnostic capabilities and by enabling condition-based maintenance for more consistent and tailored upkeep. Plus, not only are engineers putting sensors in the equipment built in shops and factories, designers are also building sensors such as strain gauges, accelerometers, and velocity sensors directly into the frames of buildings to detect structural damage and connecting them wirelessly to reduce the amount of hardware required. These embedded sensors report on the structural integrity and strength of the building itself and report the information either locally or to remote locations using the Internet. The end result of the employment of sensors, especially smart sensors, is a dynamic system of feedback and control that can sense conditions at the time of use, adapt to those conditions, and provide data for later processing. This system allows analysis of real-time data with the goal of producing smarter systems that can react to changes at a lightning pace [8]–[11].

## Biological Applications

Microsensors can also provide considerable benefits in the biomedical field for use during peacetime, wartime, or during the large gray zone between the two. For example, sensors can be used to help a person fighting infection determine medication levels or to provide continual readings on vital signs. In agriculture, the monitoring of short-term changes in fertilizer and pesticide levels or the long-term monitoring of moisture can be done using networks of wireless sensors. Especially given the current political climate, sensors that detect biological or chemical toxins and provide early warning of attacks or outbreaks can be of a great service to society. Research is under way on both inorganic sensors and organic, biological sensors that read the content levels of toxic substances and report the results over traditional wireless networks. Researchers are also looking to develop portable, automatic remote-sensing systems that can rapidly detect and diagnose biological agents. One futuristic application is sensors worn like wristwatches to provide individual sensing of chemical or biological agents. At the moment these systems are hardly portable and do not work in distributed, collaborative fashions, although the goal is to enable networked and distributed processing in the biological arena [12], [13].

While current systems are critical in cases of radiation leaks or disease contamination, the ultimate goal in sensors is to detect from within. In these cases, rather than tiny inorganic machines and computers, biological organisms would do the sensing. Organic sensors offer the attraction of integrating with the body rather than being seen as foreign, and of using power sources the body already employs. Detectors currently under development include biological tissue-based systems that measure the responses of live cells to foreign agents or toxins, those that use test molecules to detect DNA sequences or proteins, and chemical mass-spectroscopy systems that compare the DNA fingerprint or amino-acid sequence of sample agents to known bioagents or molecules [14]. Researchers in the Tissue-Based Biosensor Program at the Defense Advanced Research Projects Agency (DARPA) are investigating ways to make biosensors to detect biological agents and toxins, to assess human health risks from biotoxins, and to enhance cellular performance for agent detection and increased longevity and biocompatibility. Issues in the construction of biosensors include determination of cell-nutrient requirements, hydrodynamics and efficient transportation of nutrients and wastes, spatial arrangements of cells within a matrix, and the signal processing of electrical, optical, mechanical or other outputs from cells. Researchers are also studying detection dynamics, user interfaces, and cellular signaling for event detection and reporting [15]. However, today few of these systems are small, robust, fast, and reliable enough to qualify as microsensors except in the size of their targets. The goal is to reduce sensor size so that the sensors can be implanted in the human body and transmit such signals as chemical levels over periods of time as long as years or decades. Sensors and actuators should be able to stream through the body, dispatching medication or providing messages alerting people to the conditions of their internal workings. Applications currently under research include health monitoring (such as glucose levels and organ conditions), cancer detection, and artificial eyesight. In the case of the artificial retina, a 10x10 grid of sensors is micromachined and attached to an aluminum probe, which is then covered in a biologically inert substance. This sensor would then placed directly on the non-functional human retina, where it would produce an electrical signal resulting from light inputs. These inputs are would then be converted to a chemical signal by the tissue of the retina for eventual transmission to the brain via the optic nerve. At this time more work needs to be done on the integration of tissues with synthetic materials and the processing of the signals sent by the sensors so that the image can be more easily understood by the brain [14, p. 305], [16].

Implantable, organic biosensors are still several years away, and networks of biosensors even further. The same engineering and system-design challenges found in traditional sensor and wireless communication areas can be found in the arena of biomedical sensors, but are magnified. Low-power operation, robust and continuous operation in harsh environments, noise and topological considerations, size and weight constraints, low probabilities of detection and high probabilities of false alarms, and limited processing power all apply. The sensors will have to be robust enough to operate for years, or cheap and plentiful enough to be replaced easily. Power remains a critical issue. Work is ongoing on powering the sensors using the body itself, whether the power is derived from the motion of walking or the body's heat. And, of course, all electromechanical devices give off energy in the form of heat; how will the sensors' heat and "exhaust emissions" affect the body? Despite these challenges the body remains a fertile area for sensor usage, and researchers continue to improve sensors and actuators each day with the goal of fully integrating them into human beings [17], [18].

## Military Applications

Sensors intended for military use are distinguished not only by their applications, but also by the implications for their failure, when large numbers of lives are at stake [19]. One way to increase the chance of mission success is to keep commanders as informed as possible about enemy and friendly movements and force compositions. As a result, the military mission that benefits perhaps most from the use of sensors is reconnaissance, both long range and short range. Reconnaissance missions provide intelligence about battle spaces, or the placement and movements of friendly and enemy units; as well as about civilian personnel, the lay of the land, and other noncombatant factors. Sensors provide the raw information, which can be processed by humans or machines to eventually become useful intelligence. However, because the battlefield environment is so stressful and the penalties for failure so high, sensor systems must be designed to fuse data or perform intelligent processing and filtering to ensure that users are not inundated with too much information – or (of course) misinformation. Another mission in which sensors could benefit the military is chemical and biological weapons detection. Since soldiers face the possibility of being attacked with chemical or biological weapons, it would make sense to issue sensors directly to the soldiers in the field. Aside from biological sensors, sensors useful to the military range from air-launched, long-range acoustic sensors, to sensors towed from ships, to short-range, multiple-modality, networked sensors for insertion by personnel or unmanned aerial vehicles (UAVs) [20], [21]. To maximize useful information, especially in the case of unattended ground sensors, networks are being built so that multiple sensors can act collaboratively, with readings from multiple modalities (such as acoustic, seismic, infrared, magnetic, and visual) fused to provide one coherent signal. Sensors useful to the military must be ruggedized and have redundant systems to ensure success. To maximize the likelihood that at least some useful information will be transmitted, sensor networks for the military should be built without single points of failure, in case that a single node malfunctions or is eliminated from the network. Furthermore, networks of microsensors deployed along the ground in military missions should be mobile to account for shifting battle lines or missions, while sensors deployed in and from aircraft must account for rapidly changing atmospheric conditions and large geographic area coverage. Mobile sensors must carry their own power sources. And it is preferable for the sensors to transmit few or low power signals to avoid detection by the enemy. All these factors mean that sensors for the military must be ruggedly built, power efficient, self-organizing (which adds additional processing and power requirements), and in the case of hand-deployed sensors, small and light enough to be carried by soldiers already burdened by weapons, food, and gear [22]–[24][4].

Algorithms and technologies currently under research provide promise for sensor effectiveness in military and civilian societies in the coming years. While the use of sensors is not widespread at this time, sensors loom large in Pentagon plans for the battlespace of the future[5]. Sensors can help lift the fog and uncertainty of the battlefield by providing multispectral information with a minimum loss of life. This improvement argues for their usage, even though the technology is not always advanced enough at this stage to provide reliable readings to troops whose lives are on the line. For this reason the military comprises both the best and the worst organization in society to employ sensors: the penalties for failure are high, yet the military has the organizational and disciplinary structure to deploy and utilize sensors successfully. Plus, the military has a mission for which sensors would be clearly applicable. As a result, the military should lead the way in sensor development and use but also conduct rigorous usage and testing in peacetime environments to ensure success if sensors are used in wartime.

## Sensors and Personal Privacy

Owing to its tight disciplinary hold on its personnel, the military escapes questions about the one area of sensor usage that perhaps most troubles civilian society: privacy. Sensors offer the capability of monitoring virtually everything using technologies such as cameras mounted on small, mobile platforms and long-range, multispectral sensors capable of "seeing" thermal, acoustic, magnetic, or other types of signatures. Coupled with massive databases, powerful search engines, and faster processors, today's sensors can register an image or signature and compare it to databases for analysis and recommended action.

The implications for society are harrowing. Societies along the lines of those discussed years ago in George Orwell's *1984* and Jeremy Bentham's *Panopticon* come to mind, with people cowed into submission by the threat of constant surveillance, real or implied. Will the diminishing size of sensors and the growing power of networks and processors mean that sensors will soon be everywhere? This statement implies a technological determinism that omits people as decision-makers [25], [26]. Especially given the current trends toward acceptance of technologies, the real question should be, "Will people permit sensors to pervade all aspects of their lives?" This development is not farfetched because sensors could be seen as an antidote to crime, and because people might be afraid to oppose those segments of society interested in sensors, such as powerful industrial manufacturers or the government. Plus, pressures to accept and employ sensors would surely become even more difficult to resist as sensors become more and more pervasive [27]–[33].

In this respect sensors do not add anything new to the arguments for or against monitoring and surveillance [34], [35]. Instead, sensors make existing surveillance simpler, cheaper, and more efficient. With their wireless connections, small size, light weight, and RF communications, microsensors can provide the technology needed to make electronic networks ever more pervasive by enabling the final connections between the networks themselves and the subjects of their surveillance. In some respects this pervasiveness will be a welcome change. Remote and movable sensors can be placed at high-crime locations; infrared sensors can track personnel movements when no light is available; seismic sensors can be placed with valuable cargoes to monitor shifts in weight distribution. Sensors can extend people's eyes and ears, or present a threat of that occurring, which is often more effective than real, hidden monitoring. But this means a reduction in privacy. In effect, sensors provide the technology to erase privacy in every arena except perhaps the unexpressed thoughts of the human mind.

Indeed, while easing the minds of people performing surveillance, sensors contribute to unease of potential targets of surveillance, who could be almost anyone. By enabling remote monitoring or enabling watchers to escape notice while observing their subjects, sensors help to bring about a condition that violates personal autonomy and the principle that submission of information should be voluntary. One condition that has brought about an outcry is local governments' and police departments' use of cameras to photograph vehicles as they pass through intersections in order to catch drivers who run red lights. The American Civil Liberties Union (ACLU), which attempts to safeguard citizens' rights against unlawful or unwanted restrictions on personal liberties, has urged that this form of video surveillance be halted or delayed until privacy issues can be settled. And these arguments do not even account for troubles arising from the system's inability to accomplish its goal. Problems have arisen, such as issuing tickets to owners of cars when the owner of the automobile was not the speeding driver, or the improper use of information gained by intercepting radio frequency signals used for networked communications [36]. Will people use this and other forms of sensor technology only for benign purposes? The ACLU fears that a form of "mission creep" would occur in the use of technologies for surveillance. In other words, cameras intended to prevent traffic violations would soon be used for more intrusive ends, such as keeping databases on driver habits or watching pedestrian behavior, and would soon lead to the videotaping of all elements of society [37]–[39]. After all, while the United States has laws to prevent wiretapping and other forms of interception of voice communications using electronic media, these protections have not been expanded to include restrictions against other types of electronic monitoring. Because of sensors' small size and multiple ways of sensing the environment, the likelihood of sensors being used for other than benign reasons increases dramatically. Much as people knowledgeable in the use of the Internet feel that no information posted to or communicated via the Internet is private, sensors present the ominous condition that everything done or spoken in daily life will be open to scrutiny.

## Pros and Cons Abound

Is the role of sensors in society a foregone conclusion, especially given Americans' seemingly insatiable appetite for technological innovations [40]? The increasing processing power of computers, the connectivity provided by wireless technologies, the diminishing size of electronic components, the possibilities of completely organic sensors; and most of all, people's desires to understand and control their environments all argue that people will embrace microsensors as another means of controlling their lives or bringing enjoyment into it.

Yet sensors can facilitate centralized control, or at a minimum the loss of individual privacy. Langdon Winner proposes that artifacts themselves have political qualities, that some technologies more than others facilitate certain forms of political government or control of populations [41]. In these cases, Winner says, we ought to know the technologies better and understand the consequences of adopting their use, since the implications of adopting the technologies might be vast or unfortunate. This would seem to be especially relevant in the case of microsensors. Ideally society will examine the new "calculus of privacy" brought about by sensors and other networked elements and wrestle with the disappearance of personal privacy [42][6]. Perhaps governments and private industry groups, such as IEEE, could facilitate a debate on the use of sensors to better prepare society for the changed environment and limited privacy of a future filled with sensors. However, given people's current willingness to permit technology into so many domains of their lives, the decision to permit the intrusion might already be made.

Especially in light of recent anthrax scares and the terrorist attacks of September 11, there is an urgent need to find solutions, including technical ones, to the presence of terrorists and the possibilities of homeland violence [43]. While sensors can help to attain these objectives, it is more likely that people will embrace sensors because sensors offer something that even the networked world of current information technologies cannot offer: the possibility of intimately connecting people and the environment to computers and controls. Historians of science and technology debate whether technology drives society or the reverse. In the case of sensors, technology and society drive each other, since sensors exist at the intersection of the two.

## [Notes]

[1] The microsensors considered in this article are designed to act collaboratively in large networks without each sensor itself having much intelligence. However, many researchers are working on smart sensors and sensor agents, or devices that have the processing power to make high-level decisions and exhibit human behavior. See [1].

[2] Ember Corporation, 1 Broadway 14th Floor, Cambridge, MA 02142 (www.ember.com). The startup company aims at the market for "extremely low-cost, wireless 'thing-to-thing' networks for countless embedded processors, sensors, and controls." Another manufacturer of low-cost, wireless microsensors is Crossbow Technologies (www.xbow.com).

[3] Recent articles in the "Putting Sensors to Work" section include Carl Smith and Robert Schneider, "The Color of Money: Using Magnetic Media Detection to Identify Currency" (November 2001) and David Aslin, "Monitoring Bearing and Gear Failure in Aircraft Gas Turbine Engines" (October 2001).

[4] One research program sponsored by the Department of Defense to research these problems is the Sensor Information Technology (SensIT) Program at the Defense Advanced Research Projects Agency. See [22].

[5] See, for example, the Expeditionary Pervasive Sensors Experimental Environment (EEE). A program intended to integrate multiple sensor types and platforms, the EEE is a multi-tiered, war fighter-centered architecture of numerous and heterogeneous battlespace sensors to support a more distributed, information-oriented style of warfare.

[6] On the issue of the looming elimination of personal privacy, see issues of *New York Times Magazine*, October 7, 2001 and April 14, 2002, devoted to the subject.

## References

[1] G. Allgood and W. Manges, "Sensor agents – When engineering emulates human behavior," *Sensors*, vol. 28, Aug. 2001.

[2] P. Saffo, "Sensors: The next wave of infotech innovation," *Institute for the Future 1997 Ten-Year Forecast*, pp. 115–122.

[3] *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers,* Washington DC: National Academy Press, 2001.

[4] Alfred D. Chandler, Jr. and James Cortada, Eds, *A Nation Transformed by Information: How Information has Shaped the United States from Colonial Times to the Present*, New York: Oxford Univ. Press, 2000.

[5] B. Travis, "Sensors smarten up," *EDN Access*, Mar. 4, 1999.

[6] J. Montague, "Reaching up and out: Interface standards smarten up sensors, transducers," *Control Engineering*, Dec. 1999.

[7] R. N. Johnson, "Building plug-and-play networked smart transducers," *Sensors Mag.*, Oct. 1997.

[8] K. Mitchell, N. Dang, P. Liu, S. Rao, and H. Pottinger, "Web-controlled wireless network sensors for structural health monitoring," in *Proc. SPIE Int. Soc. for Optical Engineering*, 2001, p. 234.

[9] W. Manges *et al.*, "Intelligent wireless sensors for industrial manufacturing," *Sensors*, Apr. 2000.

[10] B. Jakoby, "Microacoustic sensors for automotive applications," in *2000 IEEE Ultrasonics Symp. Proc.*, 2000, pp. 453–460.