Context & Environmental Aware Wireless Sensor Networks for Reconfigurable Manufacturing Systems

Ivan Howitt[1], Gail-Joon Ahn[2], Teresa Dahlberg[3], Asis Nasipuri[1], Yuliang Zheng[2]

[1]Department of Electrical & Computer Engineering
University of North Carolina at Charlotte

[2]Department of Software and Information Systems
University of North Carolina at Charlotte

[3]Department of Computer Science
University of North Carolina at Charlotte

Abstract
As product cycles become shorter and the demand for customized products becomes greater, flexibility in production capabilities becomes mandatory. This trend requires manufacturing enterprises to be highly flexible with the ability to timely reallocate manufacturing resources. Wireless communications provides a natural ability to support the flexibility required by reconfigurable manufacturing systems (RMS). The formulation of a wireless communication solution for RMS will need to address issues concerning: implementation complexity, reliability and security. These issues need to be addressed in the context of the application as well as in the context of the application's environment. A framework for designing a wireless network to support the communication requirements for RMS is presented.

Keywords:
Reconfiguration, Sensor, Wireless networks

1 INTRODUCTION

As product cycles become shorter and the demand for customized products becomes greater, flexibility in production capabilities becomes mandatory. This trend requires manufacturing plants to be highly flexible with the ability to timely reallocate manufacturing resources both within a plant and across multiple plants located across the globe. In the competitive global market, plant supervisors and production managers need to maintain awareness of the production process from both aggregate production measures to modalities in an individual machine's performance. Wireless local area networks (WLAN) and wireless personal area networks (WPAN™) are poised to support these increasing demands for industrial communications. In Figure 1, a scenario is illustrated where a hierarchal wireless network is deployed. WPANs provide local communication requirements for individual manufacturing units and a broad band WLAN supports the wireless communications across the manufacturing floor. The WLAN is integrated with the corporate network. The wireless network facilitates the reconfiguration of the manufacturing units and facilitates the monitoring and control of each process either through the corporate network or by personnel on the manufacturing floor. Even though wireless communications provides a natural ability to support the flexibility required by modern manufacturing facilities, the manufacturing industry is reluctant to adopt it until the communication industry adequately addresses issues concerning: implementation requirements, reliability and security. These issues are interrelated and are interdependent. The formulation of a wireless communication solution for a specific industrial application will need to address these issues in the context of the application as well as in the context of the application's environment, e.g., manufacturing plant.

As communications becomes an integral component of the manufacturing process, the reliability of the communication network will be as important to maintain the production process as individual machines, if not more so. Likewise, compromising the security of the network could compromise the manufacturing process by directly impacting production, production quality, or by covert industrial espionage. In Section 2, we present a framework for designing a wireless network to support the communication requirements for reconfigurable manufacturing systems (RMS). Key to designing the network is understanding the RMS application

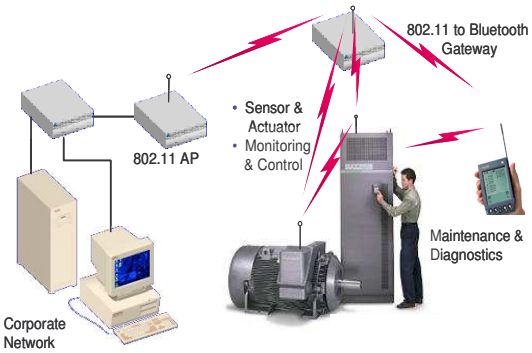

Figure 1: Industrial communication scenario for facilitating manufacturing reliability and flexibility.

requirements and the manufacturing radio frequency (RF) environment. Both of these issues are discussed further in Section 3. In Section 4, a brief overview of current wireless technologies suitable for the RMS application is presented. Specifically, the family of IEEE (Institute of Electrical and Electronic Engineers) 802.11 Standards (wireless local area networks) and family of IEEE 802.15 Standards (wireless personal area networks). Both sets of standards cover wireless devices which operate in the industrial, scientific and medical (ISM), unlicensed frequency bands. In Section 5, the paper is summarized.

2 RMS COMMUNICATION DESIGN FRAMEWORK

The use of wireless technology within manufacturing industry has been actively explored [1-3] and faces a number of challenges. This is particularly true for RMS applications. To address these challenges, a design framework for developing wireless networks for RMS is proposed as illustrated in Figure 2. The design framework is based on a cost/performance analysis. The manufacturing applications' communication requirements are mapped into three classes of cost performance constraints: security, quality of service (QoS) & survivability, and complexity & flexibility. The constraints provide a means for evaluating the trade-offs in implementing the wireless communication design in the context of the manufacturing environment.

Issues associated with the manufacturing application communication requirements and the manufacturing communication environment are presented in Section 3. Details concerning the cost performance constraints are as follows:

Security: Addresses the cost associated with the failure to prevent typically three categories of attacks on the communication network: unauthorized interception of confidential information, modification and interruption of information and network control messages.

Wireless sensor networks deployed in a manufacturing environment can be subject to both physical and logical security attacks. A deep concern to manufacturing companies is maintaining confidentiality of trade practices. Utilizing wireless technology can appear to be a potential compromise of this requirement; especially, if the wireless devices are being used to relay information pertaining to the manufacturing process. Therefore, the RMS network's capability to prevent and detect unauthorized interception needs to be evaluated. In addition, RMS networks could be subject to malicious attacks that would compromise integrity of information, as well as the availability of sensor network functions [4]. The capability to handle malicious attacks involving modification and interruption of data and network control messages [5, 6] needs to be addressed in designing the RMS network. Issues associated with risk assessment and dependency modeling for sensor networks are yet to be addressed [7]. Specifically, there is a need to identify suitable security models for interdependencies among components of a sensor network, and metrics for the measurement, analysis and comparison of risk levels. There is also a need to develop tools to evaluate the security behavior of a sensor network under malicious attacks [8, 9].

The assessment process needs to balance the tradeoff between the security requirements of the RMS communication network with the communication administration overhead associated with security protocols, i.e., security implementation cost needs to be balanced against the other two cost performance constraints.

QoS & Survivability: Addresses the ability to handle the traffic flow presented by the sensor network within the context of the manufacturing application, e.g., time latency constraints associated with the process control and/or

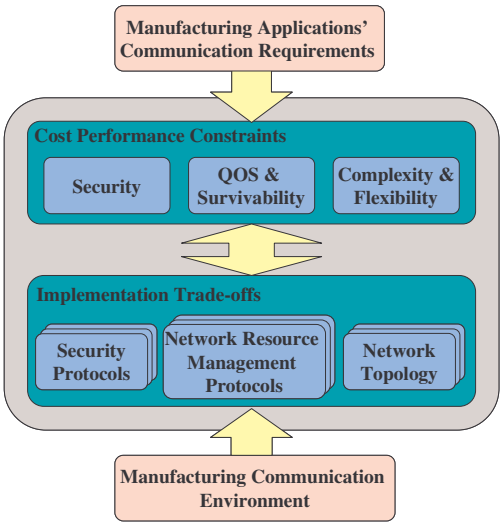

Figure 2: Design framework for developing integrated wireless sensor networks for reconfigurable manufacturing systems.

energy constraints based on battery operated sensors within the network. Also, these define the ability of the network to address communication disruptions or unanticipated variations in traffic, i.e., survivability.

QoS requirements for certain communication traffic, such as a machines servo control sensors, will have very strict requirements while others are more relaxed. Each traffic type or traffic class within the network has specific QoS and survivability requirements and the ability of the RMS network to satisfy these requirements needs to be assessed.

The focus of survivable network design [10-24] is on placement of redundant resources (e.g., links, access points, database information) and implementation of strategies to dynamically make use of these backup resources, when needed, to maintain network operations in the presence of faults. Survivability assessment is essentially a comparative cost/performance analysis of competing survivable network designs. The objective is to measure the performance of a network, in terms of the degree of functionality remaining after a failure, as well as the resultant cost of incorporating survivability. Survivable network design and analysis requires identification of a survivability objective, which can be expressed as a set of cost-performance metrics with associated parameters and constraints.

Complexity & Flexibility: Central to RMS is the ability to reconfigure the location as well as the utilization of manufacturing resources. The wireless network needs to therefore be capable of handling variations in the traffic flow due to changes in sensor location and machine utilization. The network will need to adapt to the new environment while maintaining the required levels of security, QOS and survivability. To fully enable RMS, the reconfiguration of the wireless network needs to be transparent to the end user.

3 CONTEXT & ENVIRONMENT CONSTRAINTS AND ISSUES

RMS applications present a diverse set of communication requirements and operational environments. Even though the communication requirements are diverse, there is a commonality that can be built upon in order to develop a framework for designing a communication system. This design concept is similar to the one used in cellular telephony where the design of a diverse set of wireless cellular infrastructures is based on a common design

framework [25, 26]. Within the cellular design framework, the goals are well defined, i.e., provide network access to paying subscribers at a given QoS and grade of service (e.g., blocking probability) while denying access to others. These goals are then used to design the cellular network based on using models of both the telephony traffic and the RF signal propagation environment, e.g., urban, suburban, indoor, etc. A corresponding framework can be developed for RMS communications' design. In this section, the RMS communication environment and RMS traffic are developed to provide a context for the communication system design. RF signal propagation in a manufacturing environment and potential interference sources are then discussed in order to provide a complete picture of the communication design environment.

3.1 RMS Communication's Requirements Overview

A conceptual diagram of an RMS wireless communication network is given in Figure 3. Within the RMS network there are three levels of communications: machine, machine cell (i.e., a group of machines used to manufacture a part or a subassembly) and plant floor. At the machine level, sensor data is relayed to the machine's controller. Then, aggregate data from each machine in a machine cell is collected at the cell controller which in turn is summarized and forwarded to the plant floor backbone. At the plant floor level communications, access to the corporate intranet or Internet backbone is provided. Control messages flow in the opposite direction from the plant floor backbone down to the sensors. As an example: the RMS communication infrastructure provides the means for a machine controller to change operational states based on sensor input; it allows the cell controller to coordinate the operations between machines in the cell; it provides information to the plant managers concerning the status of manufacturing operations.

RMS requires the machines in a cell to be readily reconfigured to adapt to new manufacturing requests. The degree of reconfiguration could involve modifying the usage of the current machine tools within a cell to modifying the machines comprised in a machine cell. The reconfiguration could be extended to the entire plant floor where the mix and operation of machines in each cell could be changed. Wireless technology provides a natural choice for implementing the communication network, providing the flexibility required to reconfigure the communication network when the machine cells are reconfigured.

Each level of communication has specific characteristics and requirements as discussed below.

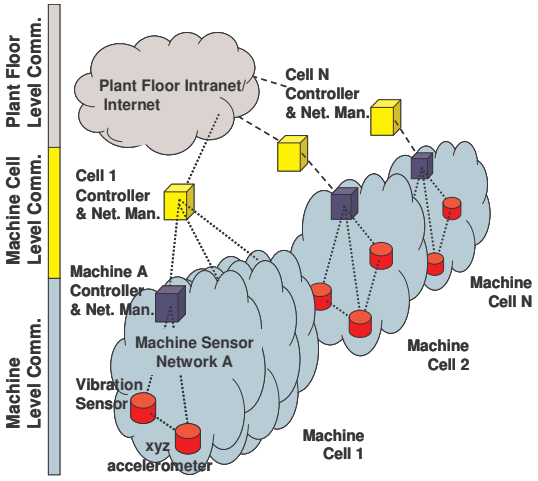

Figure 3: Reconfigurable manufacturing communication requirements overview.

Machine Level Communications

The machine level communications is handled by the machine sensor network (MSN). At the machine level, sensors are incorporated into a machine and their locations on the machine are less likely to be altered. Therefore, for the MSN, the use of wireless technology is motivated by reliability issues rather than reconfiguration issues. A principle cause of failure in machine tools is often the wire harness used to relay limit switch information to the controller [27]. Similarly, for XYZ placement devices, wiring harness failure presents a significant reliability issue [28]. Machines tools require a diverse set of sensors, with each sensor requiring a unique communication profile. A cutting machine's sensors would include thermal sensors, vibration sensors, accelerometers, and limit switches. An array of twenty or more thermal sensors is used to measure the thermal characteristics of a machine. Accelerometers provide input to the cutting head servo control and vibration sensors assist in chatter suppression [29]. Therefore, the communication traffic within the MSN is highly diverse, but it is also, for the most part, highly predictable. When a machine is operating, many sensors provide periodic updates to the controller, e.g., thermal sensors and accelerometers. The QoS required will be dependent on the type of sensor: dropping several consecutive updates from the accelerometer could cause a cutting tool servo control loop to go unstable versus the limited implication for missing several consecutive updates from the thermal sensors. Security in the MSN needs to primarily address denial of service and, to a lesser extent, unauthorized interception. The characteristics of the RF environment and the corresponding communication channel will be dominated by the machine itself, based on locations of the sensor and the machine controller. In addition, interference may be present from multiple sources including the machine or machines in the immediate vicinity as well as other wireless devices supporting communications within the machine network, machine cell networks and/or the plant floor network. Upon reconfiguring, the MSN remains fixed relative to the machine, but the traffic flow will change due to changes in machine operational requirements. Also, the RF environment will change causing the communication channel characteristics to change.

Machine Cell Level Communications

The machine cell level communications are handled by the cell sensor network (CSN). As indicated above, using a wireless device between each machine's controller and the cell controller enhances the ability to reconfigure the machine cell. This network will coordinate the operation between machine tools as well as provide a pathway for remote interrogation and control of a machine at both the cell and plant levels. At the machine cell level, the QoS will be application dependent, with machine coordination requiring a higher priority over remote interrogations. Security issues involving denial of service, unauthorized interception and unauthorized access are essential concerns of the manufacturing community. The characteristics of the communication channel will be based on the machine cell environment inside the manufacturing plant with similar interference sources as discussed at the machine level. Upon reconfiguring the machine cell, the machine cell network will need to operate based on different locations for both the machine controllers as well as the cell controller. To facilitate CSN reconfiguration, this should be carried out with minimal operator intervention.

Plant Floor Level Communications

The plant floor level communications are handled by the plant sensor network (PSN). This network provides a

pathway to allow remote interrogation and control of a cell or machine from the plant level. The QoS will be dependent on the application, but, unlike the other two levels, QoS can be improved by packet retransmission. Security issues involving denial of service, unauthorized interception and unauthorized access are essential concerns of the manufacturing community. The characteristics of the communication channel will be based on the manufacturing plant with access to the plant's intranet or Internet provided through wireless access points (AP) located typically near the ceiling of the plant. Interference is likely to be asymmetrical, since the downlink signal (signal received at the cell controller) is more likely to be impacted by interference than the uplink signal (signal received at the access point). Upon reconfiguring the machine cell, the plant floor network will need to operate based on different locations for the machine controllers using the same locations for the plant access points.

RMS Communication Traffic Generalizations

To manufacture a part, the machine tools in a machine cell are required to perform a coordinated set of predetermined operations. Based on these operations, the communications between the machine sensors and the machine controller are highly predictable. Likewise, the traffic between the machine controller and machine cell controller are, to some degree, predictable. Alarm events, such as a limit switch being tripped or thermal thresholds being exceeded, will generate traffic that is non predictable. Even though there is a high degree of traffic predictability, there is a wide range of variation in both the data rates and QoS requirements associated with each sensor's traffic. To illustrate, an accelerometer used in controlling a cutting head position requires on the order of 100 Hz update rate with 32 bits per axis resolution. Accelerometer information needs to be updated periodically within a set timing window with a high degree of reliability. Failed consecutive transmissions can lead to a catastrophic failure and using retransmissions to improve QoS is not an option due to timing requirements. An alarm event such as a thermal sensor's threshold being exceeded is a single event requiring immediate response by the controller. Successful transmission of the event is critical within a fixed time interval from the alarm's occurrence. Failure of the alarm to be successfully transmitted to the controller can again result in catastrophic failure. On the other hand, thermal sensors can be used to measure the thermal characteristics of a machine in order to adjust an operational set point and thereby improve machine performance. In this case, the update rate is on the order of every few minutes per sensor and the QoS is more relaxed. Receiving the information on a regular basis improves the machine's performance, but missing an update or using retransmission to improve QoS would be acceptable.

Understanding the RMS sensor information traffic flow is an important aspect for determining the resources and communication protocol required in designing a wireless network and in achieving the application's communication requirements.

3.2 Manufacturing RF Environment

Advances in wireless communications over the past several decades can be attributed, in part, to incorporating the evolving comprehension of the RF channel characteristics into the communication system design. By understanding the RF environment at the different communication levels, the RMS network design process and the ability to assess the design can be enhanced. In order to characterize the RMS network's RF environment, the radio signal propagation and RF interference sources need to be understood. In the RMS network, the interference sources are comprised of both environmental noise sources such as certain machine tools and collocated wireless devices.

RF Signal Propagation

Extensive work is reported in the literature on characterizing the radio propagation in indoor environments [30], including industrial sites [31-37]. This body of work provides propagation characteristics and models suitable for both the PSN and CSN. There is currently no literature found addressing the characteristics of radio propagation at the machine level, MSN.

Understanding the RF signal propagation is essential for determining: topological layout of the communication networks, interference mitigation and security issues. The maximum separation between a transmitter and receiver in order to maintain reliable communication is dependent on the environment in which the communication occurs as well as the wireless devices being used. As an example, the IEEE 802.11 WLAN specifies a frame error rate of less than 8×10^{-2} for a received signal of -80 dBm (decibels referenced to a milliwatt). Likewise, the range at which one system operating on the same frequency band may interfere with another system is governed, in part, by the RF signal propagation. From a security point of view, understanding the RF signal propagation provides insight on the locations at which RMS communication system can be compromised by either intercepted data or malicious attacks.

RF signal propagation has a natural dichotomy for characterizing its behavior due to underlying electromagnetic propagation mechanisms: large scale propagation and multipath fading. Based on an extensive measurement campaign made in five factories conducted by Rappaport [37], the large scale propagation for both PSN and CSN communication networks is well modeled by a log-normal shadowing model [26]

$$P_R(d) = EIRP + G_R + 10n\log_{10}\left(\frac{\lambda}{4\pi d}\right) + X_\sigma \ \text{(dBm)}, \qquad (1)$$

where $P_R(d)$ is the received power in dBm at a distance of d from the transmitter, $EIRP$ is the transmitter's effective isotropic radiated power, G_R is the receiver's antenna gain in the direction of the signal propagation, n is the path loss exponent, λ is the wavelength of the carrier, and X_σ is a zero mean log-normal distributed random variable (RV) with standard deviation σ. Since X_σ is zero mean, the sum of the first three terms in (1) represents the expected value of $P_R(d)$ and the received power is inversely proportional to the log of the distance where n is the proportionality constant. The RV X_σ models the variations in the received signal strength due to the variations in the obstructions between the transmitter and receiver, i.e., walls, inventory storage racks, machinery, and etc. In [37], based on a least square error fit to the entire ensemble of collected data: $n = 2.2$ and $\sigma = 7.9dB$. For individual measurement campaigns typical values of n ranged from 1.8 to 2.8 with the lognormal shadowing standard deviation ranging from 4 to 10. Figure 4 illustrates the received signal power as a function of distance based on $n = 2.2$ and $\sigma = 7.9\text{dB}$ using typical values for IEEE 802.11 operating at 2.4 GHz ($EIRP = 20\,\text{dBm}, G_R = 0\,\text{dB}$). In the figure, the shaded region represents plus and minus one sigma about the mean. Since X_σ is lognormal, the likelihood of the received signal occurring within the shaded region for a given distance is 68%.

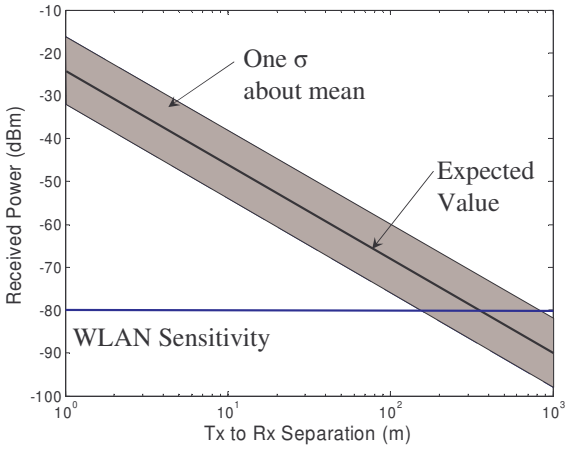

Figure 4: Received signal power versus distance based on typical values for IEEE 802.11 operating in a typical industrial environment.

As indicated above, multipath fading is another important consideration when characterizing the manufacturing RF signal propagation. Multipath fading is caused by multiple reflections of the transmitted signal arriving at the receiver. These reflections represent different wave fronts that have traveled through different paths and therefore are time delayed and phase shifted versions of the original transmission. The received signal is therefore the vector sum of these signals. Different methods can be employed to counter the effects of multipath fading. One of most straight forward methods is to use a received signal fade margin when determining the coverage range for a transmitted signal. The required fade margin can be on the order of 30 dB in an obstructed environment. This would imply using -50 dBm as the receiver sensitivity for the IEEE 802.11.

RF Interference

RF interference occurs when the detection of the desired signal is corrupted by another signal at the intended receiver. Based on current ISM band wireless protocols, data is transmitted based on packet transmissions. A corrupted packet is detected at the receiver and a retransmission is initiated. As indicated above, the impact of a corrupted signal will be dependent on the data stream affected. In order for the desired signal to be corrupted, the interference signal must occur at the same time, frequency and with sufficient power. There are two potential unintentional interference sources within the RMS Network. First, communication networks operating in the same frequency band whose operations are uncoordinated. Second, manufacturing equipment which produces harmonics within the communications networks frequency band.

Since the wireless technologies being considered for the RMS network operate in the ISM band, the potential for interference exists between various MSNs operating adjacent to each other or between the various communication layers. Methods for evaluating and designing networks which decrease the likelihood of interference between ISM wireless technologies is presented in [38-40].

In addition, certain machine tools are potential interference sources unique to the industrial environment. These interference sources include arc welders, power electronics, and induction motors. Anecdotal evidence indicates these sources of interference may be of concern, even though limited empirical data from the literature would suggest otherwise. In both [36, 37], they indicate interference from industrial noise sources is insignificant for communication systems operating above 1 or 1.6 GHz. In both cases, measurements where made at distances in excess of four meters from the noise sources. Personal computers (PC) or micro-controls are another potential source of interference. Clock speeds are near the 2.4 GHz band and could cause interference to wireless devices operating in the 2.4GHz ISM band. In order to ensure the reliability of the network operation, more details are required on the characteristics of these interference sources. This is especially true for the MSN where network devices may operate within a meter or less of interference sources.

4 OVERVIEW WIRELESS TECHNOLOGY

A significant amount of interest and application development is occurring based on wireless devices which operate in one of the unlicensed (UL) spectrums. Primary interest is for wireless devices operating in the 2.4 to 2.4835 GHz ISM band due to the international availability of the frequency band. In the US, wireless devices operating in the ISM band must operate under the FCC Part 15 rules and regulations. The FCC regulates the operation, but users are not required to obtain a license or pay license fees. The FCC limits the transmit power of the devices operating in the 2.4GHz band and thereby limits the coverage range of the device. Coverage range can be extended by two approaches: decreasing the data rate and/or by using directional antennas.

In the ISM band, a number of open and proprietary wireless standards have been and are being developed to satisfy different applications. The family of IEEE 802.11 standards [41] has become the de facto standard for WLAN. A primary difference between the 802.11 standards is the data rates supported by the standards as illustrated in Figure 5. The standards provide a wireless Ethernet like protocol with a typical network topology based on a centralized node, access point (AP), providing a link to a number of nodes, i.e., the stations (STA). To maintain reliable communications, the STA must be within the coverage range of the AP. As indicated in Section 3, coverage range is dependent on the environment in which the wireless devices operate, but the nominal indoor coverage range is 100m. The maximum data rate supported by the family of devices is 54 Mbps (802.11g & 802.11a), but this data rate is typically only achievable at a fraction of the maximum coverage range. The IEEE 802.11 family of standards can be used to support the design requirements for the PLC and MLC levels of communication within the RMS. Due to the nature of the current IEEE 802.11 protocols, the standards are less suited for satisfying the MLC requirements.

Another set of IEEE standards, IEEE 802.15 [42-44], have been developed to satisfy a different set of application communication requirements, i.e., WPAN. As indicated in Figure 5, these standards again support a wide range of data rates, but hardware complexity, cost and power requirements also differentiate these standards.

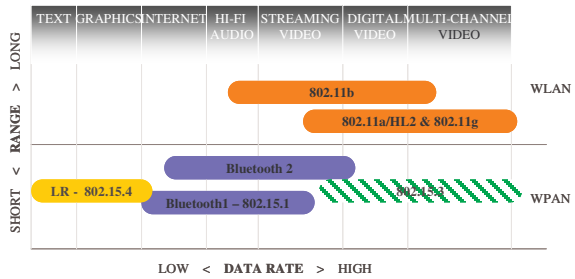

Figure 5: Current and proposed WLAN & WPAN standards.

Coverage range is typically less than 10 m. Maximum data rates range from 0.25 Mbps for the IEEE 802.15.4 to approximately 54 Mbps for the proposed IEEE 802.15.3 standard. The IEEE 802.15 devices are less suited to handle the communication requirements for the PLC due to the limited coverage range, but several strong candidates for satisfying the MLC requirements are provided.

5 SUMMARY

Wireless communications provides a natural ability to support the flexibility required by reconfigurable manufacturing systems (RMS). The formulation of a wireless communication solution for RMS will need to address issues concerning: implementation complexity, reliability and security. These issues need to be addressed in the context of the application as well as in the context of the application's environment. A framework for designing a wireless network to support the communication requirements for RMS was presented.

6 REFERENCES

[1] B. Nickerson and R. Lally, "Development of a smart wireless networkable sensor for aircraft engine health management," *Aerospace Conference Proceedings*, 2001.

[2] A. C. Weaver, "Survey of industrial information technology," *IECON'01*, 2001.

[3] P.-A. Wiberg and U. Bilstrup, "Wireless technology in industry - applications and user scenarios," *ETFA*, 2001.

[4] A.Perrig and R.Canetti, "TESLA: Multicast source authentication transform - IRTF draft," 2000.

[5] C. Pfleeger and S. L. Pfleeger, *Security in Computing 3rd*: Prentice Hall, 2003.

[6] D.Carman, P.Kruus, and B.J.Matt, "Constrains and Approaches for Distributed Sensor Network Security – Technical Report NAI Labs," 2000.

[7] A.Perrig, R.Szewczyk, V.Wen, D.Culler, and J. Tygar, "Spins: Security protocols for sensor networks," in *Proceedings of Seventh Annual International Conference on Mobile Computing and Networks*, 2001.

[8] P. Anton, "Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology - RAND Corp Technical Report, MR-1601-DARPA," 2002.

[9] C. Alberts, "Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) - Software Engineering Institute Technical Report, CMU/SEI-99-TR-017," 1999.

[10] H. Frank and I. T. Frisch, "Analysis and Design of Survivable Networks," *IEEE Transactions on Communication Technology*, vol. COM-18, pp. 501-519, 1970.

[11] R. Benjamin, "Analysis of Connection Survivability in Complex Strategic Communications Networks," *IEEE Journal on Selected Areas in Communications*, vol. 4, pp. 243-353, 1996.

[12] K. T. Newport and P. K. Varshney, "Design of Survivable Communications Networks Under Performance Constraints," *IEEE Transactions on Reliability*, vol. 40, pp. 433-440, 1991.

[13] K. Vinodkrishnan, A. Durresi, N. Chandhuk, and R. Jain, "Survivability in IP over WDM networks," *Journal of High Speed Networks*, vol. 10, 2001.

[14] A. Zolfaghari and F. J. Kaudel, "Framework for Network Survivability Performance," *IEEE Journal on Sel. Areas in Comm.*, vol. 12, pp. 46-51, 1994.

[15] T. H. Wu, "Emerging Technologies for Fiber Network Survivability," *IEEE Communications Magazine*, 1995.

[16] L. Nederlof, K. Struyve, C. O. Shea, H. Misser, Y. Du, and B. Tamayo, "End-to-End Survivable Broadband Networks," *IEEE Communications Magazine*, 1995.

[17] K. R. Krishnan, R. D. Doverspike, and C. D. Pack, "Improved Survivability with Multi-Layer Dynamic Routing," *IEEE Communications Magazine*, 1995.

[18] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Rmanathan, and J. Zao, "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions," *BBN Technologies*.

[19] C. R. Lin and M. Gerla, "Adaptive Clustering For Mobile Wireless Networks," *IEEE JSAC*, vol. 15, pp. 1265-1275, 1997.

[20] S. Ramanathan and M. Steenstrup, "A survey of routing techniques for mobile communications networks," in *Mobile Networks and Applications Journal (MONET)*, 1996, pp. 89-104.

[21] D. Tipper, S. Ramaswamy, and T. Dahlberg, "PCS Network Survivability," *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'99)*, 1999.

[22] T. A. Dahlberg, S. Ramaswamy, and D. Tipper, "Survivability Issues in Wireless Mobile Networks," in *Proceedings of First Int'l Workshop on Mobile and Wireless Communications Networks*, 1997, pp. 133-148.

[23] T. Dahlberg and J. Jung, "Survivable Load Sharing Protocols: A Simulation Study," *ACM/Baltzer Wireless Networks Journal (WINET)*, vol. 7, pp. 283-296, 2001.

[24] D. Tipper, T. A. Dahlberg, H. Shin, and C. Charnsripinyo, "Providing Fault Tolerance in Wireless Access Networks," *IEEE Communications Magazine*, 2002.

[25] W. Lee, *Mobile Communications Engineering Theory and Applications*, 2 ed: McGraw Hill, 1998.

[26] T. S. Rappaport, *Wireless Communications Principles and Practice*, 2 ed. New York: IEEE Press & Prentice Hall PTR, 2002.

[27] R. Hocken, "Personal Communication on July 24 with," I. Howitt, 2003.

[28] M. Faizullabhoy, "Personal Communication on March 2 with," I. Howitt, 2001.

[29] S. Smith and J. Tlusty, "Stabilitzing chatter by automatic spindle speed regulation," *Annals of the CIRP*, 1992.

[30] H. Hashemi, "The indoor radio propagation channel," *Proceedings of the IEEE*, vol. 81, pp. 943-968, 1993.

[31] S. Kjesbu and T. Brunsvik, "Radiowave propagation in industrial environments," in *IECON*, vol. 4, 2000, pp. 2425-2430.

[32] U. Bilstrup and P.-A. Wiberg, "Bluetooth in industrial environment," in *WFCS*, 2000, pp. 239-246.

[33] T. Rappaport, "Characterization of UHF multipath radio channels in factory buildings," *IEEE Transactions on Antennas and Propagation*, vol. 37, pp. 1058-1069, 1989.

[34] T. Rappaport and C. McGillem, "UHF fading in factories," *IEEE JSAC*, vol. 7, pp. 40-48, 1989.

[35] D. Hampicke, A. Richter, A. Schneider, G. Sommerkorn, R. Thoma, and U. Trautwein, "Characterization of the directional mobile radio

channel in industrial scenarios, based on wide-band propagation measurements," in *VTC*, 1999, pp. 2258-2262.

[36] O. Staub, J.-F. Zurcher, P. Morel, and A. Croisier, "Indoor propagation and electromagnetic pollution in an industrial plant," in *IECON*, 1997, pp. 1198-1203.

[37] T. Rappaport, "Indoor radio communications for factories of the future," *IEEE Communications Magazine*, 1989.

[38] I. Howitt, "Bluetooth performance in the presence of 802.11b WLAN," *Transaction on Vechicular Technology*, vol. 51, 2002.

[39] I. Howitt, "WLAN and WPAN Coexistence in UL Band," *Transactions on Vehicular Technology*, vol. 50, pp. 1114-1124, 2001.

[40] I. Howitt and J. A. Gutierrez, "IEEE 802.15.4 low rate wireless personal area network coexistence issues," *Proceedings of the WCNC 2003*, 2003.

[41] "IEEE standard for wireless LAN medium access control and physical layer specifications," IEEE Std 802.11-1997, 1997.

[42] "Draft IEEE standard for part 15.4: wireless medium access control(MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPANs)," IEEE Draft P802.15.4/D13, December - 2001.

[43] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mtter, and B. Heile, "IEEE 802.15.4: developing standard for low-power low-cost wireless personal area networks," *IEEE Network*, vol. September/October 2001, pp. 2-9, 2001.

[44] "Specification of the Bluetooth System v1.1," Bluetooth SIG February 22 2001.