Published in the Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Shanghai, China, 1– 4 September, 2005.

Conceptual Design and Resources for a General-Purpose Safety and Performance Verification and Validation Toolkit (V2T) for Life-Critical Wireless Medical Device Networks (WMDN)

Elliot B. Sloane, *Senior Member, IEEE* and Rick Schrenker, *Member, IEEE.*

***Abstract*— Wireless Medical Device Network (WMDN) deployment is occurring to facilitate ambulatory patient care, increase safer and more intelligent diagnostic and therapeutic capabilities, and improve flexible patient bed configuration that matches census requirements. Patient safety risks exist from delayed or lost WMDN alarm and data streams, however, and non-proprietary Verification and Validation (V2) techniques do not exist. Single-vendor and heterogeneous multi-vendor deployment must be considered, as well as safe and reliable coexistence with other IS technologies sharing similar network components. V2 of even a homogeneous single vendor, single device WMDNS is very complex for several reasons including: absence of industry standards or regulations, unconstrained mobility of patients and devices, and rapid changes in the underlying wireless network modalities. This project will evaluate and recommend appropriate best V2 practices from fields like software and systems engineering to improve a hospital's ability to properly implement and manage the emerging WMDN opportunities and to prevent patient injuries or other serious problems.**

I. INTRODUCTION

FOR the past 18 months, under the aegis of an IEEE EMBS 1073 Wireless Medical Device taskforce, senior scientists and engineers from PHS, IEEE, NIST, FCC, FDA, and manufacturers have been conferring independently and as collaborating teams on the development of a coherent framework for wireless medical devices to reliably and safely coexist. Many technical issues have come to the surface, including RF bandwidth limitations, RF signal interference, and wireless medical device network security, reliability, and performance. This international group holds weekly teleconferences and several in-person meetings each year. Invaluable leadership in this IEEE group is provided by experienced Clinical Engineers from hospitals, as well. This present paper will help address the safety and performance issues that are coming to light, and will discuss a way or organize and manage Wireless Medical Device Network (WMDN) verification and validation. The proposed process can provide significant benefits to the hospital's Information System (IS), BME and Biomedical Engineering (BME) Departments, and all affected hospital participants.

The successful creation and adoption of internationally standardized wireless data network (WDN) components based on IEEE 802.11x (a.k.a. Wi-Fi) has been a boon for users of laptop and PDA computers. Large scale adoption and manufacturing has caused prices to plummet, leading to ubiquitous deployment throughout academic, commercial, industrial, public, and home settings. This success has fed rapid existing or emerging wireless network WDN innovations including Wi-Fi (802.11a, b, and g), Wi-Max (802.11n), Bluetooth (802.15.1), and Zigbee (802.15.4) [Hampton and Wittenber, 2004]. Each of these WDNs involves trade-offs of many factors, including speed, interoperability, security, co-existence, battery life, and building/object penetration.

In the hospital setting, WDNs have many important existing and emerging business and clinical applications. Business oriented examples include supply chain management in areas like the pharmacy and operating room, patient charge billing automation, Voice over Internet Protocol (VoIP) communication, and flexible patient bed configuration for census optimization. Many clinical Wireless Medical Device Network (WMDN) opportunities exist, too, including smart infusion pumps that leverage central drug and patient knowledge banks, computerized physician order entry, mobile clinical monitoring, patient location, and point-of-care clinical diagnostic testing and patient charting. Important emerging innovations, such as the Operating Room of the Future, are likely to deploy WMDN modalities as well.

General business wireless applications (e.g., creating a purchase requisition) or archive-related WMDN applications that are not life-critical (e.g., retrieval of a mammogram) may coexist with inexpensive the common and inexpensive WDN devices, especially as available bandwidth continues to increase. To accommodate these types of multi-user data demands, an elegantly simple Collision Sense Method (CSM) is used to handle multiple simultaneous wireless messages employs random delays to re-sequence the messages. In brief, for many short-burst messages (e.g., a sentence of instant messenger text), this CSM strategy causes few visible delays, even for multiple simultaneous users. If one or more users are sending large streams of data continuous – like a 70 MByte DICOM image from radiology

Manuscript received May 2, 2005. Elliot Sloane is with Villanova University's Department of Decision and Information Systems. Villanova, PA 19085 (phone: 610-519-6432; fax 610-519-5015; email: ebsloane@ieee.org

Rick Schrenker is the System Engineering Manager in the Biomedical Engineering Department of Massachusetts General Hospital, Boston, MA (email: raschrenker@partners.org).

– the all other users will likely experience noticeable erratic delays in system response.

Life-critical applications present very serious challenges and patient risks, however [Hampton 2004, Cypher 2004]. The unpredictable CSM delay can easily extend beyond the AAMI/ANSI-specified 10-second critical heart alarm period [AAMI/ANSI 2002] Furthermore, the randomization of message transfers can completely invalidate intelligent alarm system management such as that specified in IEC/ISO 60601-1-8.

In addition, erratic delay in real-time patient waveforms interferes with computerized and human interpretation, causing misdiagnosis of illnesses and/or interfering with therapeutic interventions. Also, erratic WMDN-induced delays can cause intermittent spurious alarms such as lead-loss or missing patients, reducing system trust and greatly increasing "no problem found" complaints and investigations for the IS and BME departments and the manufacturers.

II. Statement of Opportunity:

Simulations of WMDN signal traffic have already been created using a set of well proven and very sophisticated software tools known as Petri Nets (PN) and Colored Petri Nets (CPN) [Sloane and Gehlot 2004 & 2005, Gehlot 2004]. Sloane and Gehlot (2005) demonstrate CPN for a small WMDNs supporting 20-40 devices. The CPN software uses a simple graphic interface that allows rapid modular customization and reconfiguration. Recent papers illustrate how the CPN simulation can be used to detect WMDN problems for any particular configuration. When properly configured to match the planned or existing WMDN, this tool can be used for pre-purchase system V2 planning. Furthermore, this tool can support future expansion planning, as well as later-stage problem identification and resolution.

The CPN simulations cannot, by themselves, ensure safe and reliable in-situ WMDN operations because real-life situations are too complex. For example, a single hardware or software upgrade or repair to one medical device or network component can introduce a new hidden failure mode for the device or the whole system. In other cases, ambulatory patients congregating for therapy, training, or meals may overload WMDN nodes. Unfortunately, this problem will be compounded when clinical and operations staff use their own wireless devices for tasks like RFID inventory location, hand-held appointment scheduling, or VoIP telephone services. Last, as mentioned earlier, ever-growing clinical file transfer opportunities (e.g., DICOM MR, CT, X-Ray, Nuclear Medicine, Ultrasound, and other images) can effectively disable improperly configured WMDNs.

Radio-frequency (RF) signal problems can, and do, can cause unique WMDN challenges in several ways, too. Many of the IEEE- and FCC-specified frequencies are unfortunately shared by other technologies, including appliances and wireless phones. Many consumer products, like cell phone headsets, games, and PDA's have built-in Wi-Fi or Bluetooth systems already, and one can expect that Zigbee and other modes will follow in time. Unfortunately, many of the frequency and signal modulation techniques are known to disrupt each other, limiting the number of simultaneous devices that can be safely supported [Cypher 2005]. Furthermore, physical plant challenges, like steel and concrete structures and RF-emitters like radio stations, motors, and high-power electronic devices, may necessitate unique receiver and antenna configurations.

An astute reader will likely conclude that such problems are not solely found in healthcare. IEEE's wireless standards program does have a Quality-of-Service (QoS) protocols that is known as 802.11e. In general terms, this QoS standard does define an method of providing improved wireless message performance for high-priority messages. In fact, many manufacturers do claim to include a QoS component in their WMDN designs. Unfortunately, several critical problems are not solved. Standardized QoS hardware and software has not yet achieved broad industry acceptance, resulting in a proliferation of incompatible proprietary solutions. In addition, even the IEEE 802.11e standard was not designed with life-critical messages in mind, and there is not way to ensure that such wireless signals are transferred with 100% certainty.

Two other factors undermine current QoS solutions: ubiquitous diffusion of WDN throughout many commercial and personal devices and many WMDN vendor's reluctance to share responsibility for safe WMDN performance if other vendor's products are attached. Even if a hospital wanted to, it can rarely consider surrendering all of its WDN and WMDN to a single vendor because no single vendor supports all necessary business and clinical applications.

It should be clear that hospitals must have a way to safely and reliably integrate and manage a broad selection of wireless medical, industrial, and personal devices with a necessarily limited number of wireless access points. Therefore, this project focuses on development of a Verification and Validation Toolkit for WMDN systems.

This project will mutually benefit the IS and BME departments, and it will help both hospital groups ensure safe, reliable, and efficient WMDN system selection, deployment, and support

III. Components for the Verification and Validation Toolkit

The goal of this activity is to develop a prototype Verification and Validation Toolkit (V2T) that will allow the Biomedical Engineering and Information Systems departments ensure safe and reliable operation of WNDN [Cypher 2005, Hampton 2004 & 2005, Sloane and Gehlot 2005]. Regardless of the careful planning and procurement management that goes into selecting and installing such

systems, there are, by nature, many intentional and unintentional ad-hoc changes that can occur throughout the life cycle of these systems. Furthermore, because the distribution of Decision Support System (DSS) capabilities for life-critical analysis of ECG arrhythmias or drug interactions varies by manufacturer, model, and user configuration, no single validation strategy can, by itself, universally assure safe and reliable WMDN systems.

One important component of this Toolkit may well include the creation of a usable Color Petri Net (CPN) WMDN simulation tool for planning and change management. Sloane and Gehlot [2005] have already developed a prototype WMDN model using CPN to simulate a small system of heart and pulse oximetry monitors wirelessly connected via a Wi-Fi network to a central nursing station. Simply explained, the CPN model allows testing the state of each component in the network by tracking the movement of each packet of information (called a 'token'). The strength of CPN (i.e., beyond basic, non-color Petri Net tools) is that each token can be color-coded, and each component in the system can be programmed with special decision rules for each token. In the Sloane and Gehlot model, both standard Wi-Fi and 802.11e QoS, priority-rule-based message management has been simulated. The CPN software includes a programming language that can be used to force a life-critical heart alarm like ventricular fibrillation (v-fib) to move to the head of other wireless message queues. This ensures ensuring the fastest possible transit through the network.

Any life-threatening alarm like v-fib can be assigned a color (red, for example), and lower priority data (orange, yellow, green, blue, etc) can each be handled by different rules at any point in the network. Every colored token can be monitored throughout the network, and data on transit times, delays, and dead nodes or deadlock conditions can all be saved in an Excel or SPSS file for analysis.

The CPN software also has a graphical interface which allows modules to be copied and/or customized as needed. Because of this, we believe it can be used to quickly represent almost any patient monitoring configuration (i.e., almost any number and configuration of patient monitors, wireless network hubs, and central stations, along with accurate priority and decision rules). Unlike any other existing tool, this CPN model can allow pre-planning of WMDN by including appropriate components and network element, and rules, and then running simulations to detect problems like insufficient bandwidth, inadequate priority management, deadlock conditions, and unreachable states. Note that this model does NOT simulate or test the RF environment. Transceiver interference or physical problems like shielded walls are not addressed. The important contribution, then, is that this CPN model CAN assure that when the RF issues are addressed, the WMDN will function properly. Further, as future changes to the WMDN are planned, the existing model can be updated and retested.

A usable V2T will also provide a way to validate the safe and reliable initial and ongoing performance of each WMDN system, and to do so, it must document and test all alarm functions, clinical data management, and any other operational data that is included.

Three general verification and validation techniques exist (NIST 1997), often referred to as:

1. Black box testing – unknown internal system components or configuration that requires through external testing of all functions and potential failure modes to determine reliability.
2. White box testing – complete internal system details fully known and transparent for testing and observation, which allows complete systemic performance testing.
3. Gray box testing – hybrid situation of Black and White box systems, in which only some internal detail and access is available.

It is expected that the prototype V2T will have to include all three approaches, as some portion of both heterogeneous (mixed vendors and/or models) and homogeneous systems will have hidden (unknown) interactions that must be validated regardless of the situation.

In the case of a complete system installation, a formal, independent validation process is desirable. This would allow installation acceptance testing as well as periodic systemic revalidation following major system repairs or changes. In keeping with IEEE Software Engineering practices, a validation process such as this can be performed incrementally: first validating individual pieces or modules and then validating subsystems by careful testing of all interface modes and functions. Ultimately, the entire system is validated by testing the combination all subsystems. Manufacturer testing or verification procedures must be considered during this process, but they are rarely site- or situation-specific, and they are often out of date.

Once a complete WMDN system is successfully validated, safe and reliable system performance following individual changes, such as repairing a device or upgrading a piece of hardware or software should be verified and documented by testing critical performance parameters and/or anticipated critical failure modes such as power interruptions. Again, if available, manufacturer documentation may be helpful for portions of this work.

A prototype V2T methodology will need the following processes and related documentation:

1. Detailed inventory of each device, subsystem, and interface;
2. Identification and selection of appropriate detailed white-, black-, or gray-box testing technique for each device, subsystem, and interface;
3. Creation of a verification process and documentation package that specifies all tests and results;

4. Determination and documentation of verification intervals and/or criteria;
5. Creation of preliminary verification process and documentation for future repairs, upgrades, and changes; and
6. Periodic review of verification and validation procedures and documentation.

IV. Conclusions

This proposed V2T will serve the following critical risk mitigation functions following any WMDN component or system change:

1. Assure patient safety
2. Assure reliable system operation
3. Assure detection of problem states
4. Assist in diagnosis of problems
5. Assure HIPAA compliance
6. Meet JCAHO alarm management requirements

The risks inherent in creating such a toolkit lie in development and deployment of an inadequate or grossly inefficient V2T. If the V2T is incomplete or inaccurate, it could lead to a false sense of security and, potentially, to selection, installation, and acceptance of expensive WMDN systems that have unacceptable failure or safety characteristics. Further, if the V2T is too complex or grossly inefficient, it may not be practical for any but the most complex and/or expensive projects.

At present, however, no suitable general alternative exists in the market. Vendor-specific validation and verification procedures are rarely fully documented as a matter of proprietary protection. In addition, the vendor will rarely accept any responsibility for customization or mixing other vendor's products with theirs, creating an unacceptable sole-vendor deadlock.

V. References

[1] AAMI/ANSI EC13:2002 Standard for Cardiac Monitors, Heart Rate Meters, and Alarms

[2] Cypher, National Institute of Standards (NIST) February 2005, 802.11x and 802.15x Incompatibility Analysis for the IEEE 1073 Wireless Medical Device Taskforce.

[3] Gehlot. 2004. Timed Petri Nets, Linear Logic, and Performance Modeling. Proceedings of the 2004 International Conference on Modeling, Simulation and Visualization Methods.

[4] Hampton. 2004. CE Challenges. AAMI Annual Clinical Engineering and Productivity Subcommittee Meeting. June4, Boston, MA.

[5] Hampton. 2005. Report at IEEE 1073 Wireless Medical Device Working Group at the FDA. March, Gaithersburg, MD.

[6] IEEE Software Engineering Standard(s) and/or book(s)?

[7] IEC/ISO/DIS 60601-1-. 2003 Medical equipment – Part 1-8. General Requirements for safety – Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems.

[8] National Institute of Standards and Technology (NIST). 1996. Reference Information for the Software Verification and Validation Process (http://hissa.ncsl.nist.gov/HHRFdata/Artifacts/ITLdoc/234/val-proc.html)

[9] Sloane and Gehlot. 2005. Colored Petri Net Simulation for Design of Heterogeneous, Multi-Vendor, Integrated, Life-Critical Wireless (802.x) Patient Care Device Networks. Accepted for the Americas Computer and Information Society (AMCIS) 2005 Annual Conference, July 2005. Omaha, NB.

[10] Sloane and Gehlot. 2004. Applications of the Petri Net to Simulate, Test, and Validate the Performance and Safety of Complex, Heterogeneous, Multi-modality Patient Monitoring Alarm Systems. Proceedings of the IEEE Engineering in Medicine and Biology Annual Conference, September, San Francisco, CA.

[11] Wittenber. 2004. Wireless network standard overview for IEEE 1073 Wireless Medical Device working group, as cited in Hampton, 2004, above.