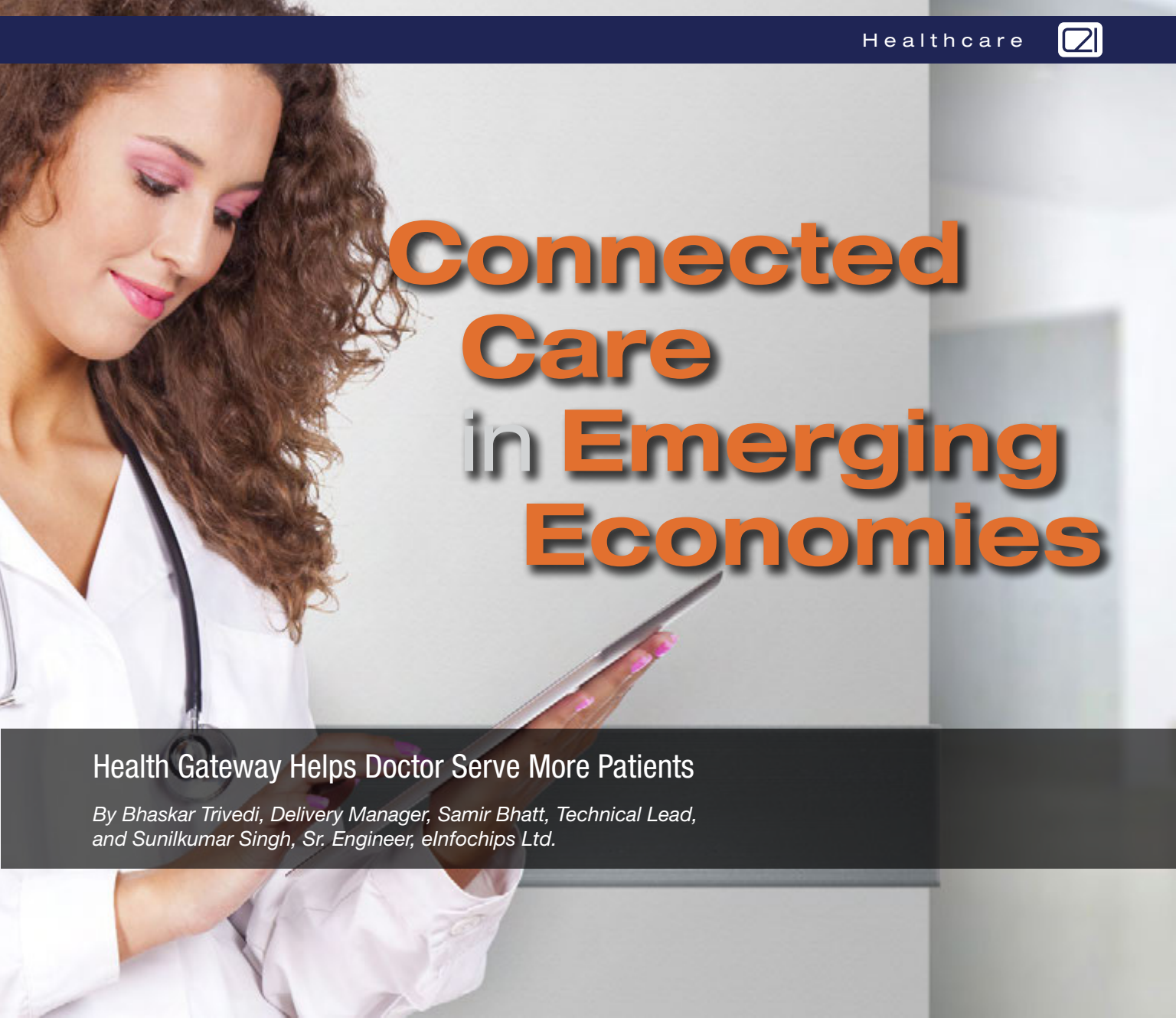

Connected Care in Emerging Economies

Health Gateway Helps Doctor Serve More Patients

By Bhaskar Trivedi, Delivery Manager, Samir Bhatt, Technical Lead, and Sunilkumar Singh, Sr. Engineer, eInfochips Ltd.

In emerging economies, access to healthcare services is limited and expensive. Consider doctor-to-patient ratios: Afghanistan has only 2 doctors for every 10,000 patients, India has 6, China has 18, the United States has 24, and Switzerland has 41 (Source: World Bank, 2010 data). To address this discrepancy, doctors in developing countries need tools to help them prioritize time among patients and deliver care efficiently.

Connected care technologies are bridging this gap by giving doctors remote access to patient data. In this article, we present an example proof of concept (PoC) based on the Intel® Quark™ processor. The PoC aggregates patient data and uploads it to the cloud, allowing doctors to analyze patient needs and optimize their schedules accordingly. What's more, the PoC can be transformed into a low-cost, production-ready design with minimal time and effort – thus creating an effective solution for developing economies.

Delivering Connected Care

Connected care solutions leverage the Internet of Things (IoT) to connect medical sensors to the cloud, enabling automated monitoring of vitals like temperature, blood pressure, pulse, and respiration. Doctors can use the data to estimate patient conditions and prioritize visits to patients that need maximum attention. Automated alerts can be created so the doctors can take preventative measures and address issues before they become critical. Attendees are freed from making periodic measurements that may be prone to human errors. Medication schedules can be monitored to ensure continued health. Patients can even be released from a hospital early and have their conditions tracked while they go about their normal lives.

Together, these benefits can go a long way towards addressing healthcare issues in emerging economies. Medical staff can make the best use of their time and patients get reliable access to critical care. The result is a significant improvement in patient outcomes that keeps costs under control.

To meet these goals, however, a connected care solution faces several challenges. First and foremost, the solution must be affordable for emerging economies. It must be offer excellent battery life and a small form factor to encourage consistent use. Excellent reliability and security are also critical so that the solution can ensure safe, continuous operation; minimize technician visits; and protect patient information. Above all, the solution must offer excellent connectivity to sensors as well as to the cloud through cellular or Wi-Fi*.

Healthcare Proof of Concept

To illustrate how developers can create an effective connected care solution, eInfochips developed the PoC shown in Figure 1. As an initial use case, the PoC monitors a patient's temperature and notifies medical staff when it exceeds certain limits. Key components of the PoC include:

- Portable and low-cost ZigBee* sensors for data collection and aggregation
- Sensor processing software based on Yocto Project Linux*
- A sensor aggregation unit and wireless gateway based on the Intel® Quark™ SoC X1000
- Wi-Fi and 3G/4G cloud connectivity
- Cloud infrastructure built on the Amazon platform for record keeping and reliable storage
- Mobile access to patient data through PCs or mobile platforms
- Automatic alerts at various levels of criticality with a call to action

Sensors can be connected wirelessly using various means such as Bluetooth, Wi-Fi, or ZigBee. eInfochips chose ZigBee for our PoC because it enables efficient operation for battery-powered devices. ZigBee sensors can be powered by coin cells and have minimal weight and size. ZigBee supports a secure "mesh" network topology that adds robustness to the solution. Medical devices typically use the ZigBee Health Care (ZHC) profile of the ZigBee Standard. ZHC supports the ISO/IEEE 11073 protocol that makes it interoperable with other compliant ZHC devices, simplifying the overall device network infrastructure.

The output of these wireless sensors is aggregated at a common junction, a gateway powered by the Intel® Quark™ SoC X1000. Intel, along with the Intel® Internet of Things Solutions Alliance, has developed a range of gateway solutions that come pre-integrated with software from Wind River and McAfee – who are both Associate members of the Alliance. These pre-validated solutions help ease the burden of deploying low-cost intelligent gateways. Some of these solutions are based on Intel Quark SoC X1000 and others are based on Intel® Atom™ processor E3800 product family. We will look more closely at these gateways later in this article.

As illustrated in Figure 2, the eInfochips PoC gateway can securely communicate with the cloud through Ethernet, Wi-Fi, or 3G/4G. The data from cloud can be made accessible to registered and authenticated users like the patient, doctors, nurses, and pharmacists. This data can be accessed continuously (in case of proactive healthcare), or on an as-needed basis.

The Heart of the Solution

The Intel Quark SoC X1000 at the heart of the PoC plays a key role in creating a low-power, low-cost remote patient monitoring system. As shown in Figure 3, the system on chip (SoC) is highly integrated, incorporating multiple peripherals for sensor and network connectivity. These include multiple GPIO inputs to enable connection of analog sensors like passive infrared (PIR) and ultrasonic sensors.

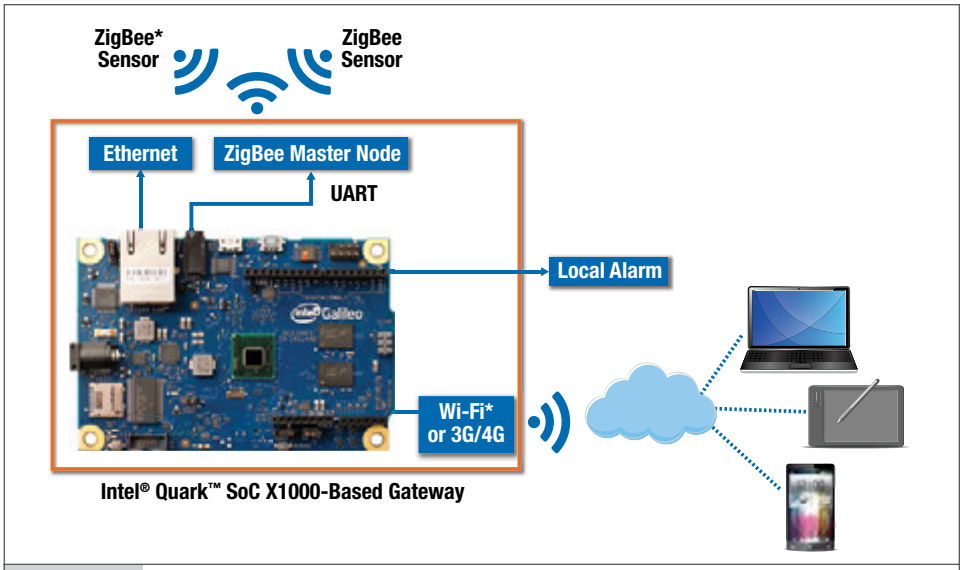

Figure 1. The proof of concept shows how to deliver efficient care.

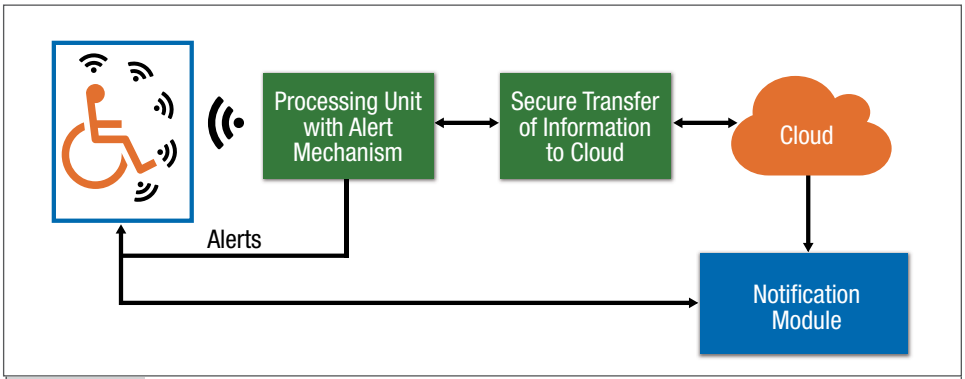

Figure 2. The solution integrates cloud infrastructure for remote monitoring.

Building these interfaces into the SoC significantly reduces the bill of materials (BOM) for patient monitoring infrastructure and personnel. The high integration and 15 mm x 15 mm package also reduce the overall size of the solution. Power consumption is also minimized, as typical power consumption is 1.5 W with a maximum thermal design power (TDP) of 2.3 W.

The SoC smartly addresses security and reliability as well. A Secure Boot on-die ROM on many SKUs enables endpoint and content security, ensuring that only chosen software runs on a device. Pre-boot vulnerabilities can be further avoided by reserving the part of the memory for data and code execution – a feature called Execute Disable (XD). In addition, extended temperature (-40 °C to +85 °C) and DDR3 memory with error-correcting code (ECC) options provide a high level of data integrity.

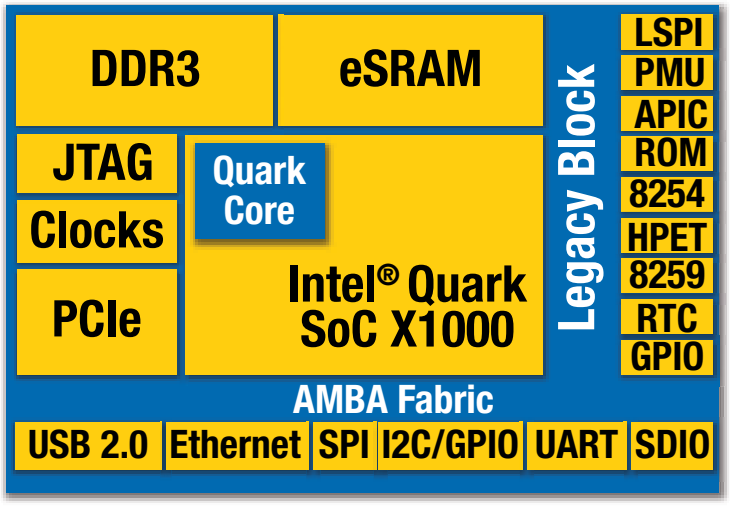

Figure 3. The Intel® Quark™ SoC X1000 is highly integrated.

These security features are important for embedded system design. Embedded systems are vulnerable to a range of exploitations that can expose private information, drain the power supply, destroy the system, or hijack the system for uses other than its intended purpose. Security is doubly important in healthcare, where patient data requires safeguarding not only during transfer but also within the end devices. Vulnerability at the end user device, like easy access to the security keys used to encrypt or decrypt data, can easily expose the patient information.

Speeding Time to Market

Intel Quark SoC X1000 is available as part of the Intel® IoT Gateway. These gateways are designed to simplify and speed development by pre-integrating off-the-shelf software including Wind River* Linux, the Wind River* Intelligent Device Platform (Wind River* IDP), and McAfee*