BAND-AiDe: A Tool for Cyber-Physical Oriented Analysis and Design of Body Area Networks and Devices

AYAN BANERJEE, SAILESH KANDULA, TRIDIB MUKHERJEE, and SANDEEP. K. S. GUPTA
IMPACT Lab, Arizona State University

Body Area Networks (BANs) are networks of medical devices implanted within or worn on the human body. Analysis and verification of BAN designs require: i) early feedback on the BAN design; and ii) high-confidence evaluation of BANs without requiring any hazardous, intrusive, and costly deployment. Any design of BAN further has to ensure: i) the *safety* of the human body, i.e. limiting any undesirable side-effects (e.g. heat dissipation) of BAN operations (involving sensing, computation, and communication among the devices) on the human body; and ii) the *sustainability* of the BAN operations, i.e. the continuation of the operations under constrained resources (e.g. limited battery power in the devices) without requiring any re-deployments. This paper uses the Model Based Engineering (MBE) approach to perform design and analysis of BANs. In this regard, first, an abstract cyber-physical model of BANs, called BAN-CPS, is proposed that captures the undesirable side-effects of the medical devices (cyber) on the human body (physical); second, a design and analysis tool, named BAND-AiDe, is developed that allows specification of BAN-CPS using industry standard Abstract Architecture Description Language (AADL) and enables safety and sustainability analysis of BANs; and third, the applicability of BAND-AiDe is shown through a case study using both single and network of medical devices for health monitoring applications.

Categories and Subject Descriptors: C.4 [**Performance of Systems**]: Modeling techniques; I.6.4 [**Model Validation and Analysis**]: ; I.6.5 [**Model Development**]: ; J.3 [**Life and Medical Devices**]: Medical information systems

Additional Key Words and Phrases: Wireless Health Systems, Body Area Networks, Model Based Engineering, AADL

1. INTRODUCTION

Recent developments in wireless technology, pervasive computing, and wearable and implanted electronics have led to the development of Wireless Health Systems (WHSs). One of the key components of WHSs is Body Area Networks (BANs), which are generally *wireless networks* of medical devices capable of sensing, actuation, computation, and communication among themselves. The devices can be either wearable on the human body [Korhonen et al. 2003; Paradiso et al. 2005; Mistry et al.] or implanted [Schwiebert et al.], (`http://circ.ahajournals.org/cgi/content/full/105/9/1022`). BANs have a wide variety of use for WHSs in various

Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.
© 20YY ACM 0000-0000/20YY/0000-0001 $5.00

applications such as personal health monitoring applications [Milenković et al. 2006; Venkatasubramanian et. al. 2005] and specialized physiological data gathering systems used by medical practitioners in hospitals (`http://www.smithsoem.com/`). This paper deals with the design and verification of BANs to meet different WHS requirements.

1.1 Motivation

Real deployment may include device implantation and faulty BAN operations may harm the human body. Thus, verification of BANs under real situations can be highly intrusive, hazardous, time-consuming, and costly. As such, it is imperative to perform automated design and verification of BANs that can provide credible feedback at early design phases, without requiring any actual deployment [Sandeep, K.S. Gupta 2009]. An efficient way to perform such design and analysis of a system is the Model Based Engineering (MBE) approach. In this approach, the designers build models or abstractions of systems' behavior and perform analytical evaluations on the model to verify different design decisions. Such an approach can allow the International Regulatory Agencies (IRAs), e.g. the Food and Drugs Administration (FDA), to perform fast approval of BANs for use. FDA indeed has been involved in applying MBE to validate various requirements of medical devices before market approval [Weininger et al.]. This paper uses MBE to perform automated design and verification of BANs.

1.2 Challenges and Requirements

BANs are inherently *cyber-physical* in nature, i.e. the operations in the cyber entities (medical devices) can affect the physical environment (human body) and vice versa. Interactions between the medical devices and the human body have to be considered in designing and verifying BANs to avoid any undesirable behavior. For example, recent studies have shown that the headphones' electro-magnetic fields can interfere with the heart pacemakers within a specific range to produce wrong stimulus (`http://www.medicaldevicesafety.org/`). Proper behavioral modeling of the pacemakers, which capture such interactions, along with the analysis of their operations could have identified the design flaw before any actual deployment. Interactions between the BAN devices and the human body can be of two types:

(1) ***Intentional* interactions**: These interactions are required for the BAN functionalities. Monitoring the physiological signals by a medical device, e.g. heart rate by EKG, and actuating medical actions, e.g. infusing insulin in the human body by insulin pump, are examples of intentional interactions.

(2) ***Un-intentional* interactions**: These interactions are the undesirable side-effects of the BAN operations on the human body and vice-versa. For example, heat dissipation from the devices can undesirably cause temperature rise in the tissue. Similarly, tissue growth can reduce the devices' sensing and communication ranges; thus, affecting the BAN operations.

The un-intentional interactions can potentially harm the human body. For example, studies show that operating a pulse-oximeter probe at 44°C for eight hours can cause skin burns [Greenhalgh et al. 2004]. The problem gets exacerbated if there are aggregate effect from multiple devices on the same part of the human tissue.

The *Medical Electrical Equipment Standard* puts a limit on the devices' operating temperature (e.g. 41°C for pulse-oximeter probes (IEC 60601-1-6 Ed. 1.0 b:2004 standard)). Any operations (including, sensing, computation, and communication) in the medical devices therefore has to ensure that the resulting heat dissipation (and potential aggregate effect) does not cause a temperature rise beyond such limits for human safety. Another major challenge is the resource constrained nature of the medical devices in BANs [Banerjee et al.]. In general, the duration of the BAN operations are limited by the battery capacities in the medical devices. The following list summarizes the design requirements of BANs:

—**Safety**: The non-intentional interactions with the physical environment (e.g. heat dissipation) has to be within a pre-defined limit.
—**Sustainability**: BAN operations has to be designed such that power consumption is reduced and alternate green power sources (i.e. supplementary to the battery power) from the human body (e.g. ambulation, respiration, etc.) [Paradiso and Starner 2005] are used to sustain the BAN operations without any re-deployment.
—**Security**: The information exchange among the medical devices should maintain privacy, authenticity, and integrity of the personal health data. Indeed the Health Insurance Portability and Accountability Act (HIPAA) mandates securing all electronically transferred health information (`http://www.hhs.gov/ocr/hipaa/`). To this effect, our previous work has focused on extracting cryptographic keys from the physiological signals, sensed by the devices [Venkatasubramanian et al. b]. Ensuring security generally involve complex cryptographic operations requiring considerable resources (CPU cycles, memory, battery power) in the medical devices. Therefore, there is an inherent trade-off with sustainability and even safety since the device power consumption directly determines the heat dissipation.
—**Accuracy and Low latency**: The BAN design should guarantee correctness of BAN functionalities since any failure can potentially cause medical emergencies. This can be achieved by ensuring that all the intentional interactions occur correctly. A generic framework to model and analyze the intentional interactions in Cyber-Physical Systems (CPSs) has been developed in [Karsai and Sztipanovits]. Further, any delay in BAN operations should be low because of the applications' time-critical nature (e.g. health data transfer during emergencies). Modeling and analysis of Wireless Sensor Networks (WSNs) behavior have been performed in [Prasad et al.] to ensure accuracy and low-latency. However, ensuring a high degree of accuracy and low latency may increase the computational burden on the medical devices; potentially trading off the BANs' safety and sustainability.

This paper focuses primarily on the safety and sustainability requirements and proposes MBE for BANs to meet these requirements. In this regard, first it is imperative to properly model the un-intentional interactions for safety analysis of the BANs. Secondly, appropriate modeling of the intentional interactions can aid in the sustainability analysis by properly capturing the energy scavenging from the green sources. Thirdly, low resource usage and latency of BAN operations need to be analyzed as part of the sustainability analysis. Further, it is also important to note the challenges associated with modeling and analysis of BANs. First and foremost,

the abstract model has to be: i) *simple*, allowing easy modeling of BANs to ensure usability; ii) *analyzable*, ensuring that the safety and sustainability analysis can be computationally feasible; and iii) *uniform*, so that a single software platform can be used for specification and analysis of both the computing and physical aspects of BANs[1].

1.3 Goal and Contributions

The goal of this paper is *to perform MBE to design and analyze BANs in terms of the safety of human body during the BAN operations and sustainability of these operations*. To this effect, the main **contributions** of the paper are:

(1) *Abstract model of BANs as CPSs (BAN-CPS)* that captures both intentional and un-intentional interactions between networked medical devices and the human tissue.
(2) *Body Area Networks and Devices – Analysis and Design (BAND-AiDe)* tool that enables specification of BAN-CPS and analyzes BANs' safety and sustainability.
(3) *Case studies* demonstrating the design and analysis of BANs' safety and sustainability in wireless health monitoring applications using BAND-AiDe.

1.4 Overview of Approach and Results

BANs are modeled in BAN-CPS as a combination of two types of components: 1) the cyber components (corresponding to the medical devices); and 2) the physical components (corresponding to the human body). The physical components are abstracted as enclosing regions of the human body around the medical devices with which the the devices interact. In this regard, two types of modeling abstractions, *Region-Of-Interest (ROIn)* and *Region-Of-Impact (ROIm)*, are proposed for the intentional and un-intentional interactions, respectively. The boundary of the ROIn and ROIm are determined by the computing properties (e.g. sensing range and communication range) and physical properties (e.g. extent of heat dissipation) of the medical devices, respectively. Further, the ROIn and ROIm are inter-dependent with each other. For example, increasing the communication and sensing range can increase the device power consumption; thus, increasing the heat dissipation. Similarly, tissue growth (change in ROIm) can affect the sensing and communication ranges of the devices. A single medical device with its ROIn and ROIm is termed as a Local CPS (LCPS). A collection of LCPSs constitute a Global CPS (GCPS) that maps a BAN to the BAN-CPS model.

Intersections between ROIms of multiple LCPSs represent aggregate side-effects of the operations in the LCPSs' devices. For example, the temperature rise in the intersecting ROIms is an additive effect of the heat dissipation from the multiple devices whose ROIms intersect. The BAND-AiDe tool uses the BAN-CPS model to analyze BANs' safety and sustainability. The sustainability analysis is performed by evaluating the power extracted from the ROIns. Current design of BAND-AiDe allows thermal safety analysis that involves verifying if the temperature rises in the ROIms are within the thermal safety limits. The worst-case complexity of the analysis in BAND-AiDe is $O(n^2)$, where n is the number of medical devices.

[1]Merely integrating domain specific tools to perform separate analysis on the two aspects of CPSs will require users to be familiar with the respective tools separately.

Currently, the industry standard Abstract Architecture Description Language (AADL) is used to specify the BAN-CPS model. In this regard, the AADL is extended through the development of a BAN-CPS annex. The annex allows specification of: i) the physical dynamics in the human tissue, normally determined by differential equations (e.g. Pennes' bio-heat equation [Pennes 1948] to determine temperature rise); and ii) the ROIns and ROIms. These specifications were not supported in the AADL standard language (`http://www.aadl.info/`). Safety and sustainability analysis were performed by developing analysis plug-ins in the OSATE analysis platform (`http://www.aadl.info/`) for AADL models. The usage of BAND-AiDe is demonstrated through a case study which includes safety and sustainability verification of: i) a single high-power pulse-oximeter device; and ii) a network of low-power medical devices. In this regard, a secure health monitoring application, Ayushman [Venkatasubramanian et. al. 2005], is used that consists of sensing, communication, and physiological value based security [Venkatasubramanian et al. b] operations.

1.5 Paper Organization

The rest of the paper is organized as follows. Section 2 provides the related work on MBE in general and associated design tools for embedded systems, WSNs, and CPSs. Section 3 discusses the preliminaries on BANs and an overview on MBE. Section 4 presents the BAND-AiDe tool including the BAN-CPS model, analysis techniques for safety and sustainability, and AADL based implementation. Section 5 provides the case-study followed by a discussion on the broader impacts of BAND-AiDe in Section 6. Finally, Section 7 concludes the paper.

2. RELATED WORKS

WHSs have been one of the main application areas of embedded computing research for the past few years and a number of realizations of such systems exists. These systems include small individual wireless medical devices such as pulse oximeters (`http://www.smithsoem.com/`) or camera capsules (`http://www.rfamerica.com/sayaka/index.html`) as well as a network of medical devices on human body [Milenković et al. 2006; Venkatasubramanian et. al. 2005]. Previous research on safe and sustainable BANs have focused on: i) developing multi-hop cluster-based communication scheduling algorithms that ensure thermal safety of the human body [Tang et al. 2005]; ii) analyzing the sustainability of sensing and data dissemination operations in BANs [Park et al. 2008]; and iii) designing sustainable information security protocols for inter-device communications [Venkatasubramanian et al. a]. However, all these approaches are application-specific. A generic methodology to design and verify safe and sustainable BANs is missing. This paper fills this gap by performing MBE of BANs.

Figure 1 depicts the modeling requirements of BANs, maps the related work to address the specific modeling requirements, and puts the contributions of BAND-AiDe into perspective. There are three basic modeling requirements for BANs: i) cyber entities, i.e. the application software (e.g. health monitoring software) and networked computing units (e.g. embedded medical devices), ii) physical environment, i.e. the human body, and iii) interactions between the physical environment and the cyber entities (both intentional and un-intentional). Intentional interac-

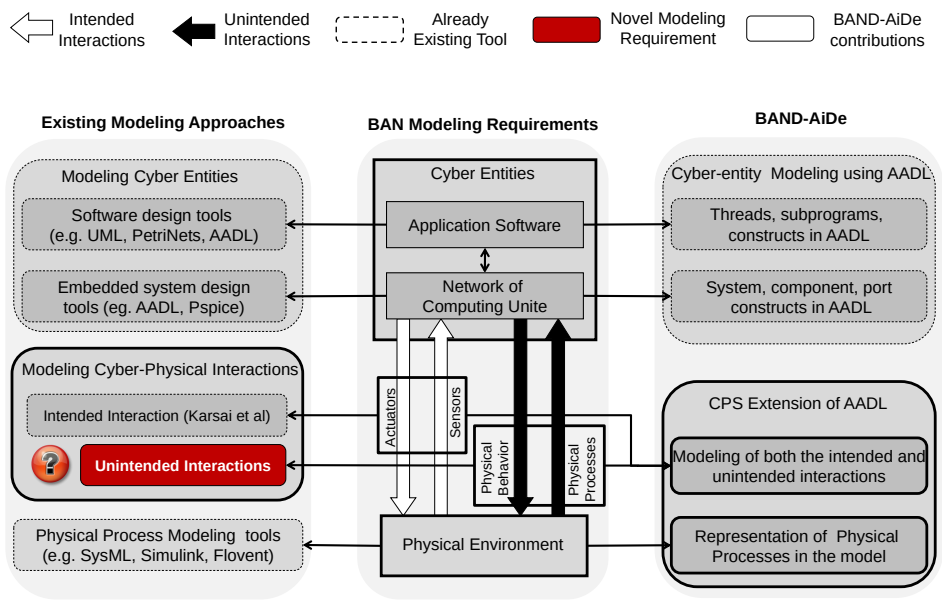

Fig. 1. BAND-AiDe contributions

tion modeling would involve sensor and actuator behavior modeling. Un-intentional interaction modeling requires modeling the physical processes and the physical behavior of the cyber entities.

MBE has been widely used for embedded systems. A large number of tools are available that model and analyze hardware of computing systems such as Pspice [Tuinenga 1991] and AADL (`http://www.aadl.info/`), and application software such as UML (`http://www.uml.org/`) and Petrinets [Elena and José 2006]. The authors in [Prasad et al.] have proposed a tool called *ANDES* that introduces the concept of MBE in WSNs to ensure accuracy and low latency of WSN operations. The MBE approach is also used to study the behavior of physical systems through tools such as SysML (`http://www.sysml.org/`), Simulink (`http://www.mathworks.com/`), and Flovent (`http://www.mentor.com/`). However, none of these tools can model the cyber-physical interactions. A generic framework to perform MBE of CPSs has been proposed in [Karsai and Sztipanovits]. However, the framework only considers the intentional interactions for the proper functioning of the CPSs. MBE of BANs further need to consider the un-intentional interactions to analyze BANs' safety and sustainability. The proposed BAND-AiDe tool provides a uniform model specification and analysis platform that addresses all the three salient modeling requirements for MBE of BANs.

3. PRELIMINARIES

Before presenting the BAND-AiDe tool in the next section, this section provides a brief overview on BANs and the MBE approach.

3.1 Body Area Networks (BANs)

A Body Area Network (BAN) is a heterogeneous set of medical devices that can sense, actuate, compute, and communicate with each other through a wireless chan-

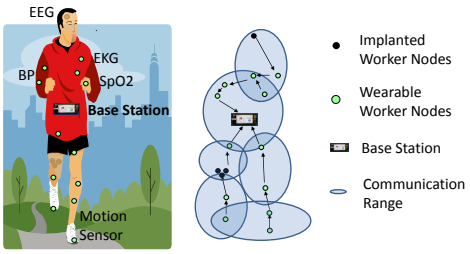

Fig. 2. Body Area Network

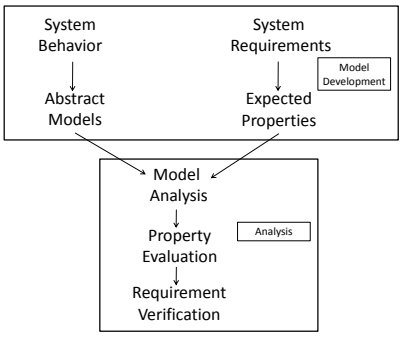

Fig. 3. Model based engineering methodology

nel. These medical devices are henceforth referred as the *nodes*. The envisioned architecture of BAN is shown in Figure 2. The nodes in a BAN can be broadly classified into two categories: 1) *worker nodes*, which are implanted or wearable medical devices with a low computing capability interfaced with sensors, actuators, and wireless transceivers (e.g. a PPG sensor interfaced with TelosB motes); and 2) *base station*, which has higher computation and communication capabilities (e.g. PDA) to disseminate and collect information to and from the worker nodes, respectively. Each node in a BAN has a set of neighboring nodes with which it can communicate through an one-hop wireless link (indicated by the communication range in Figure 2). A BAN can be either single-hop, i.e. the base-station is a neighboring node of all the worker nodes, or multi-hop, i.e. the base-station can be reached by a worker node (and vice versa) through multiple intermediate nodes (Figure 2). The following subsection provides a brief overview on MBE methodology before it is applied for BANs in Section 4.

3.2 Model Based Engineering (MBE) Methodology

MBE is the method of developing behavioral models of real systems and analyzing the models for requirement verification. Figure 3 depicts the different phases in this methodology. There are two main phases in MBE: 1) model development, and 2) model analysis. In the model development phase, a set of *expected properties* of the system is determined from the *system requirements*. An abstract modeling is further performed that generally involves capturing appropriate parameters whose variations can reflect the *system behavior*. Mathematical analysis (*model analysis*) is then performed on the abstract model to *evaluate* the expected properties and *verify* the system requirements. The goal of this paper is to use MBE in designing and analyzing BANs, a key component of WHSs, and introduce a tool, called Body Area Networks and Devices Analysis and Design (BAND-AiDe), that enables abstract modeling of BANs as CPSs and allows analysis of the model to verify safety and sustainability of BANs.

4. BAND-AIDE: ANALYSIS AND DESIGN OF BODY AREA NETWORKS

This section presents the BAND-AiDe tool. Figure 4 shows the architecture of the tool and depicts how it enables the execution of the different phases in MBE. As shown in the figure, BAND-AiDe consists of a model development framework, called the *BAND-AiDe Modeling Framework* (Section 4.1), and a model analysis engine, called the *BAND-AiDe Model Analyzer* (Section 4.2).

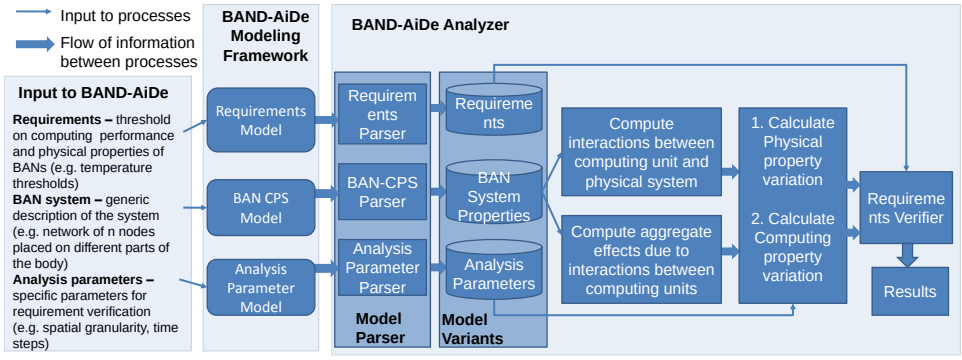

Fig. 4. BAND-AiDe tool architecture

4.1 BAND-AiDe Modeling Framework

The modeling framework helps in the model development phase of MBE (Figure 3). There are three inputs to the framework:

(1) **BAN Requirements**: These are usually a set of limits or thresholds on the system parameters (Section 1.2). For example, an upper limit on the maximum body temperature (system parameter) ensures safety. Similarly, for BAN sustainability, the requirements are to ensure that at least a given number of nodes (system parameter) can be operated using available power from different energy resources.

(2) **BAN System**: This includes BAN deployment information such as the number, types, spatial distribution, and communication topology of the nodes.

(3) **Analysis Parameters**: These are specific parameters for the model analysis. Example of such parameters include time steps, spatial granularity of differential equation solvers (e.g. Finite Difference Time Domain (FDTD) [Tang et al. 2005]), and functions determining the aggregate effects (e.g. summation function to combine heat effects from multiple computing units).

Given these inputs, the following subsections describe modeling methodologies in the BAND-AiDe modeling framework.

4.1.1 *Requirements Modeling.* The thresholds on the system parameters, which characterize the BAN requirements, can be modeled in BAND-AiDe by providing a set of **constants**. These constants will be used in the requirements verification phase to check if the BAN behavior is suitably constrained.

4.1.2 *Abstract Modeling of BANs as CPSs (BAN-CPS).* This modeling methodology is used on the **BAN System** inputs to model BAN behavior. BAND-AiDe envisions a BAN as a CPS, which consists of a set of computing (i.e. cyber) components (medical devices) and a physical environment (human body). Figure 5 shows a typical deployment of the BAN nodes including both implanted and wearable (i.e. on the skin) worker nodes. Both the intentional and un-intentional interactions are further depicted in the figure. This CPS view of BAN is termed as BAN-CPS. Figure 6 shows all the modeling constructs of BAN-CPS in a hierarchical form. Following are the modeling constructs:

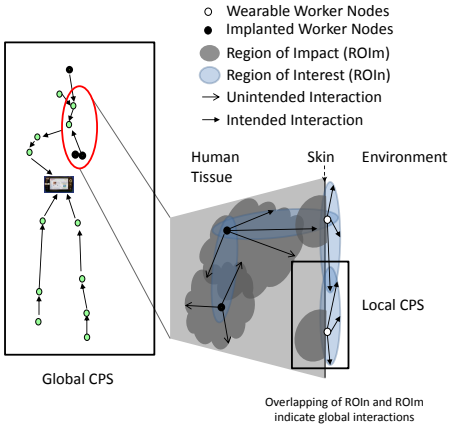

Fig. 5. BAN-CPS: BAN as a Global Cyber-Physical System (CPS).

Global CPS (GCPS): A BAN is considered as a GCPS (Figure 5), i.e. a collection of distributed and networked cyber-physical subsystems. Each of these subsystems consists of a single worker node. The GCPS construct can also correspond to the portion of the physical environment observed for analysis, e.g. the portion of human body monitored by BANs.

Local CPS (LCPS): Each individual subsystem in a GCPS is referred to as an LCPS. The LCPS construct models each worker node in BANs as a single CPS. This enables modeling and analysis of the interactions between each individual node and the physical environment in a modular fashion. Each LCPS consists of three types of constructs:

—*Computing unit*: This construct corresponds to the worker nodes capable of sensing, computation, and communication. The construct facilitates the modeling of both computing and physical behavior of the worker nodes through the following two properties:

  —*Computing property*: This property characterizes the computing behavior, e.g. the processor speed of a worker node or the amount of memory space available. The computing properties depend on the hardware configuration of the computing unit and the design of the application software. The hardware and the application software should be designed such that BAN operations are accurate and have low latency. These design requirements have been addressed in [Banerjee et al.] and are out of the scope of this paper. Trade-offs between these design requirements with safety and sustainability are demonstrated in the specific case studies (Section 5).

  —*Physical property*: This property characterizes the physical behavior, e.g. the power dissipation, of the computing unit. These properties often depend on the computing behavior of the nodes and can cause un-intentional interactions. For example, the processor speed determines the power dissipation of the worker nodes. This in turn causes un-intentional temperature rise of the human body.

—*Physical unit*: This construct is used to model the portion of the physical environment with which the computing unit interacts. These interactions usually affect the system parameters, for which the thresholds are provided in BAN

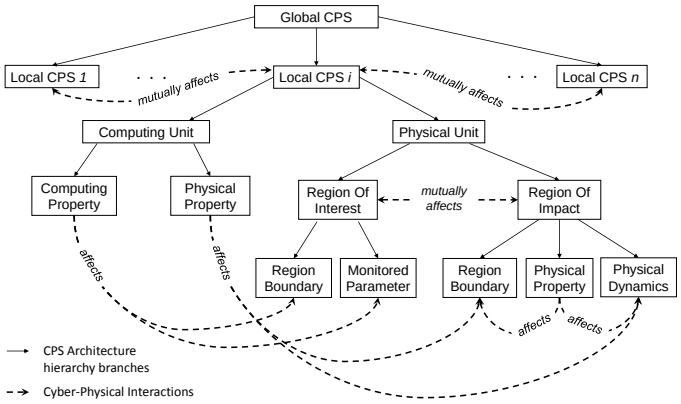

Fig. 6. Hierarchical view of the generic constructs to model BAN-CPS.

requirements. For example, the heat dissipation (un-intentional interaction) from the nodes affects the body temperature (system parameter). The modeling paradigm of BAND-AiDe hypothesizes that **any interaction of the computing unit with the physical world will take place within a bounded region**. Therefore, all interactions are limited within a region defined in the LCPS. To this effect, two types of regions for intentional and un-intentional interactions are specified in the physical unit. These regions are described below:

—*Region-Of-Interest (ROIn)*: This construct facilitates the modeling of the intentional interactions, e.g. the sensing and the wireless communication region. A ROIn has two attributes:

  —**Monitored parameter**: This construct models the system parameters that are affected by the intentional interactions. For example, the physiological signal sensed by a worker node can be a monitored parameter, which is affected by the nodes' sensing capabilities (electro-magnetic interaction [`http://www.quasarusa.com/`]).

  —**Region Boundary**: This attribute represents the limits of the bounded region, within which the intentional interactions are confined. The region boundary depends on the variation of the monitored parameters. For example, when the sensed signal is the monitored parameter, the sensing range of the worker node becomes the region boundary.

—*Region of impact (ROIm)*: This construct is used to model the un-intentional interactions. The ROIm consists of three attributes:

  —**Physical Property**: This attribute characterizes the physiological parameters such as blood glucose level, blood pressure, tissue temperature etc. These properties depend on the location of the node, physiological conditions, and environmental factors such as temperature, pressure etc (`http://urwhatueat.org/carb5.html`).

  —**Physical Dynamics**: This construct enables modeling the physical processes. These processes are normally expressed in terms of complex equations. For example, the process of body temperature variation is governed by a partial differential equation [Pennes 1948].

  —**Region Boundary**: This is similar to region boundary in ROIn. However, the

region boundary of ROIm depends on the physical properties and dynamics. Since the physical dynamics are governed by differential equations, the region boundary can be specified by boundary conditions on the equations. These conditions are generally limits on the physical properties outside the ROIm. For example, in case of temperature rise in human body, we can assume that the body temperature is 37 °C outside the ROIm. We can then employ this boundary condition to the associated differential equation [Pennes 1948] to obtain the region boundary.

—*Local Interactions*: The local interactions are cyber-physical interactions between the computing unit and the physical unit within an LCPS (denoted by the dashed lines in Figure 6). The intentional and un-intentional interactions are modeled using the following constructs, respectively:

—**Intended interactions**: These are modeled as transfer of information between the computing unit and the ROIn. For example, the sensing of physiological signals from the human body by a node can be modeled by this construct.

—**Unintended Interactions**: These interactions as modeled as transfer of energy between the computing units and the ROIm. For example, heat transfer from the computing unit to the corresponding ROIm can be modeled by this construct.

Note that an interaction is also defined between the ROIn and the ROIm of an LCPS. These are used for representing certain special cases, where there are inter-dependencies between the ROIn and ROIm, as described in Section 6.

Interactions among the LCPSs: In the BAN-CPS model, interactions between different LCPSs can also take place. For example, the wireless communication between two worker nodes in a BAN is a form of information transfer between two different LCPSs. This phenomenon can be modeled by introducing the concept of interconnections between the LCPSs. These interconnections are called *global interactions* (as depicted by the two way dashed arrows in Figure 6). Global interactions between two LCPSs normally occur whenever there is an overlap in the ROIn or the ROIm of the two (as shown in Figure 7). This notion of global interaction facilitates the modeling of a network of nodes in a BAN (through overlapping of the ROIns) or the cumulative thermal effect of the nodes on a particular area of the physical environment (overlapping of the ROIms). Global interactions can be intended or unintended due to the overlapping of the ROIns or ROIms of the interacting LCPSs, respectively.

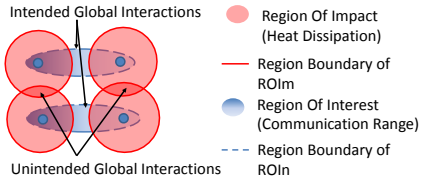

Fig. 7. Global Interactions

4.1.3 *Analysis Parameter Modeling.* Analysis of a model generally involves specific methodology to solve equations that govern the physical dynamics. The solution techniques often require a configuration, i.e. assigning values to certain specific parameters determining the quality of the solutions. For example, solving the Pennes' equation will require the FDTD time and space discretization approach. The granularity of such discretization can be specified in the model as sets of *constants*. Further, the aggregate functions can be specified as a set of equations

```
Process:    BAND-AiDe  Analyzer (BAND-AiDeModel)

Model Parser   /* Parse model and extract the Model Variants */
GCPS = Model Parser(BAND-AiDeModel.BAN-CPSModel);
[Performance Thresholds]  = Requirements parser(BAND-AiDeModel.RequirementsModel);
[Analysis Parameters] = Analysis Parameter parser(BAND-AiDeModel.AnalysisParametersModel);

Interactions between computing unit and physical system
for each i from 1 … n
   GCPS.LCPS(i).ROIm.Physical Property = EvaluatePhysicalProperty(GCPS.LCPS(i).ROIm, AnalysisParameters)
for each i from 1 … n
   GCPS.LCPS(i).ROIn.Monitored Parameter = EvaluateMonitoredParameter(GCPS.LCPS(i).ROIn, AnalysisParameters)

Interaction between different computing units
for each i from 1 … n
      for each j from 1 … n
           if GCPS.LCPS(i).ROIm.RB overlap with GCPS.LCPS(j).ROIm.RB
            IntFm(i,j) = 1;
           else
            IntFm(i,j) = 0;
           if GCPS.LCPS(i).ROIn.RB overlap with GCPS.LCPS(j).ROIn.RB
            IntFn(i,j) = 1
           else
            IntFn(i,j) = 0;
for each IntFm(i,j) == 1
      GCPS.LCPS(i).ROIm.Physical Property  = Compute the aggregate effect in the intersecting region;
      GCPS.LCPS(j).ROIm.Physical Property  = Compute the aggregate effect in the intersecting region;
for each IntFn(i,j) == 1
      GCPS.LCPS(i).ROIn.Monitored Parameter  = Compute the aggregate effect in the intersecting region;
      GCPS.LCPS(j).ROIn.Monitored Parameter  = Compute the aggregate effect in the intersecting region;

Requirements Verification
for each Param.time step
      for each Param.space step
           Compare Monitored Parameter with performance thresholds
Return Verification Results
```

Fig. 8. Pseudocode for BAND-AiDe Analyzer

combining the physical dynamics of different LCPSs.

4.2 BAND-AiDe Analyzer

The BAND-AiDe analyzer determines the BAN behavior from the BAN-CPS model. The behavior is then verified against the requirements given as input to the BAND-AiDe modeling framework. Figure 4 shows the work flow of the BAND-AiDe analyzer.

The models from the BAND-AiDe modeling framework are first parsed into a suitable format by a **Model Parser**. There are three different components of the parser: 1) requirements parser, 2) BAN-CPS parser, and 3) analysis parameter parser. Each of these components correspond to the three modeling aspects of the modeling framework (Section 4.1). The output of the *Requirements Parser* is a set of constants indicating the thresholds on different system parameters. *Analysis Parser* provides parameters (a set of constants) related to the analysis methodology (e.g. configuration for equation solvers, time step and spatial granularity). The *BAN-CPS Parser* extracts the hierarchical organization of the BAN-CPS model in a structure using which interactions and aggregate effects can be computed. The outputs of the parsers are called the *Model Variants*.

The pseudocode of the analyzer is shown in Figure 8. The *EvaluatePhysicalProperty* and *EvaluateMonitoredParameter* routines evaluate the variations of the physical properties and monitored parameters within the Region Boundaries (denoted by RB) of the ROIm and ROIn of each LCPS, respectively. These evaluations essentially compute the local interactions within an LCPS. Note that the represen-

tation of the Region Boundary by the notation GCPS.LCPS(i).ROIm.RB reflects the hierarchical nature of the constructs (Figure 6). Similar notations for the other constructs are also used.

The next process is to identify and compute the interactions between different computing units. This process involves the computation of the global interactions. In the pseudocode, this is achieved by iterating through all n^2 possible pairs of LCPSs (where n is the number of nodes in the BAN) and checking whether the RBs of LCPS pairs overlap. These overlapping regions are tracked by the parameters, IntFm and IntFn, for ROIm and ROIn, respectively. The aggregate variation of the physical properties and the monitored parameters are then evaluated for these regions of intersections. To this effect, the aggregation functions provided in the analysis parameter model are used.

After computing the interactions and aggregate effects, the analyzer checks the monitored parameters and the physical properties against the requirements. This process is called the requirements verification process. The results of the verification process are compiled to generate an analysis report.

4.3 Implementation

Given the modeling framework and the analysis work flow in the previous subsections, this subsection presents the current implementation of BAND-AiDe. The modeling framework of BAND-AiDe is developed using the Abstract Architecture Description Language (AADL). AADL is an industry standard language to model real time embedded systems and is suitable for implementing BAND-AiDe due to the following reasons:

—AADL specifications are hierarchical in nature, which helps in specifying the BAN-CPS model.

—AADL has dedicated construct to model hardware and software of embedded computing devices. This will be helpful in modeling the behavior of the computing units in the BAN.

—AADL has been used to model wireless sensor networks [Prasad et al.]. This modeling is directly applicable for the BAN computing units.

—AADL provides facilities for language extension through development of annexes. These facilities can be used to incorporate the generic constructs of the BAN-CPS model in AADL.

A description of the AADL constructs used in this paper is given in Appendix A.1.

4.3.1 *Model Specification.* The GCPS in the BAN-CPS model (Figure 6) can be represented using the *system* construct in AADL (as shown in Figure 9) and is named **Global CPS (GCPS)**. In the GCPS, the monitored region of the human body is specified as a grid. The origin and the units of the grid are specified using the *properties* construct. The constants for the requirements specification and the analysis parameters can be provided in the GCPS specification using separate *property sets*, which are AADL constructs to specify system attributes. The **GCPS** consists of several *subcomponents* called **Local CPS (LCPS)**. These are also modeled using the *system* construct. Each **LCPS** consists of three *subcomponents*: 1) **Computing Unit**, which models a single worker node, 2) **Region of Interest**, which models the ROIn, and 3) **Region of Impact**, which models the ROIm. The

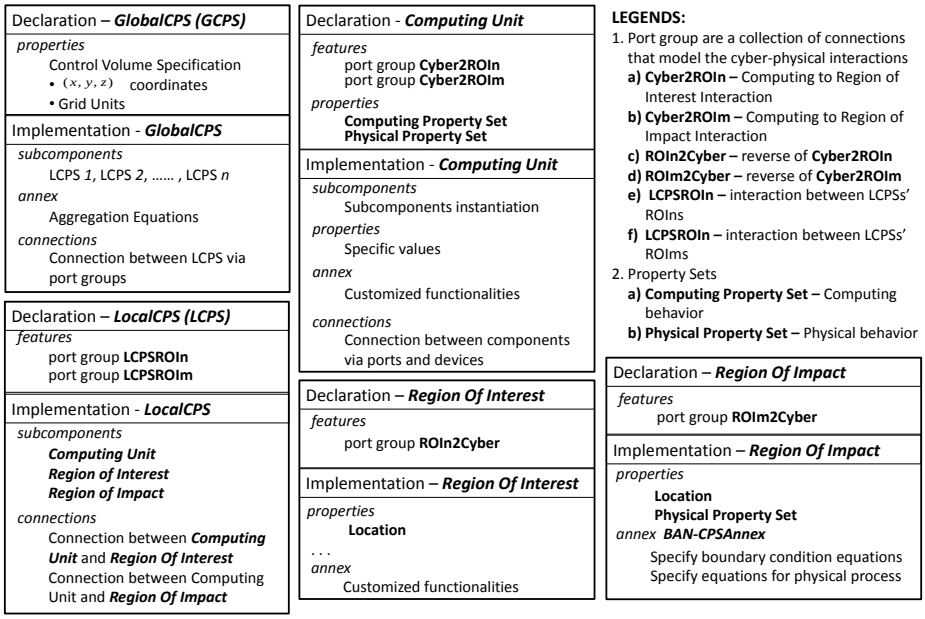

Fig. 9. AADL specification of the BAN-CPS model

system construct is used to model these subcomponents. The **Computing Unit** has two *property sets*, **Computing Property Set** and **Physical Property Set**, to model its cyber and physical behavior, respectively. The **Computing unit** can be modeled in a conventional way, containing *subcomponents* such as processor, memory, radio, and bus [Prasad et al.].

The location of the worker node is specified using the **Location** *property set*. This property set gives the coordinates of the worker node with respect to the origin and grid units defined in the GCPS. Within an ROIm, the worker node is considered to be the origin. The ROIm consists of properties from the **Physical Property Set**. The dynamics of the physical system which involves specification of complex analytical expressions is specified with the help of the **BAN-CPSAnnex**. This *annex* extends AADL with customized constructs for specification of partial differential equations. The **Region Boundary** of the ROIm is represented by boundary conditions on the properties of physical unit. Similar approach is taken to implement the ROIn of the LCPS.

The global and local interactions in the BAN-CPS model are specified with the help of *port group* AADL construct. The *port group* construct is an assembly of different types of *port*s. These *port*s, along with their interconnection using the *connections* construct, models information transfer among the subcomponents. The **Computing Unit** has two *port groups*: 1) **CyberToROIn**, which specifies the *intended interaction* of the computing unit with the ROIn and 2) **CyberToROIm**, which specifies the unintended interaction of the computing unit with the ROIm. The global interactions are modeled using two types of *port groups*, **LCPSROIn** and **LCPSROIm**, in each LCPS. These *port groups* signify interactions between a

computing unit of an LCPS and the ROIn and ROIm of some other LCPS, respectively.

4.3.2 *Analysis framework.* The analysis framework is developed on the OSATE platform, which supports AADL model specification and analysis through java plug-ins in eclipse. The analysis framework uses the parsers provided by the OSATE platform to parse the AADL constructs. A new parser was developed for the customized differential equation constructs in the **BAN-CPSAnnex**. In BAN-CPS Annex specific constructs were declared for denoting differential equations. The construct $DeltnXY$ represents the mathematical operator $\frac{\delta^n X}{\delta^n Y}$. The differential equations were then parsed using the following context free grammar:

```
Operator = Variable * DeltnXY * Operator + Variable * Operator |
           Variable * DeltnXY * Operator - Variable * Operator | null
DeltnXY = Delt1XY | Delt2XY ..................
Variable = any string | null
```

The parsed differential equations are represented in the form of a parse tree. In the Analysis plug-in, the parse tree representation of the equations was converted into a mathematical form. Currently, the BAN-CPS Annex converts the parsed equations into FDTD form which can be solved using any FDTD solver. To this effect, the analysis plug-in is integrated with domain specific tools such as Matlab. The analysis results were provided in a graphical format through Matlab.

5. CASE STUDY FOR DESIGN AND ANALYSIS WITH BAND-AIDE

This section shows the usage of the BAND-AiDe tool to model and analyze BAN operations. To this effect, we consider: i) a BAN with wearable and implanted worker nodes, and ii) a secure health monitoring application, Ayushman [Venkatasubramanian et. al. 2005]. The worker nodes are assumed to be capable of:

—sensing temperature, humidity, sound, and physiological signals (e.g. Photo-Plethysmogram (PPG));

—data communication through wireless radio; and

—communication security through Physiological value based Key Agreement (PKA) [Venkatasubramanian et al. b].

Figure 10 shows the Ayushman workload highlighting the three operations. As shown in Figure 10, the operations in the worker nodes have different CPU utilization profile. These utilization profiles determine the nodes power consumption. Hence, proper duty-cycling and communication scheduling can be employed to reduce the nodes' power consumption. The nodes are assumed to be always expending the maximum power, P_c, if duty-cycling is not employed. On the other hand, when duty-cycling is employed, then the nodes do not always consume maximum power. In such a case, the power consumption of the sensor node when radio is turned off is given by P_{proc}. During the communication operation, the processor consumes P_{proc} amount of power. The radio transmitter will also be active during this operation (P_{radio} being its power consumption). In a single day, there will be x number of sense and transmit periods (sleep cycles) for each worker node in the BAN, with a duration of $(t_s + t_{Tx})$ seconds each, where t_s and t_{TX} denote the time required to perform the sensing and communication operations, respectively..

Table I. Available Scavenging Power

Scavenging Source	Available Power (W)	Scavenge Time (Hrs)
Body Heat	0.1 - 0.15	24
Ambulation	1.5	2
Respiration	0.42	6
Sun Light	0.1	3

The symbol t_{PKA} denotes the duration to execute the PKA. The total number of nodes is assumed to be n, and the nodes execute pairwise PKA (once everyday) to ensure freshness of keys. In PKA, frequency domain features are derived from the sensed physiological signals and are used to facilitate key agreement between two sensors. The feature extraction process involves several complex computations such as Fast Fourier Transform (FFT) and peak detection. The node power consumption during the PKA operation is comprised of the power required for the aforementioned computation, P_{PKA}, and the power required to keep the radio on, i.e. P_{radio}. For simplicity, thermal effects are considered for maximum node power consumption. Thermal safety verification under this worst case situation guarantees thermal safety in all other situations. However, duty cycling is considered for sustainability verification to analyze the improvement in the number of nodes, sustained by the energy scavenging sources.

We consider the presence of four stand-alone scavenging sources from which the nodes can be powered: 1) body heat, 2) respiration, 3) ambulation, and 4) sun light. Table I lists the amount of available power and the hours of scavenging operation considered for each scavenging source. These scavenging sources are supported by storage units that store the scavenged energy. The nodes are assumed to be equipped with actual energy-scavenging devices [Gyselinckx et al. ; Park et al. 2008] or inductive charge transfer devices [Chen et al. 2008] to enable charging from the storage units. To obtain the model parameters for BAND-AiDe through experimental evaluations, Ayushman was implemented in a BAN consisting of TelosB motes interfaced with temperature, humidity, and physiological sensors. The implementations were performed to meet the design requirements of accuracy and low latency. Figure 11 shows the implementation strategy of the peak detection stage of the PKA protocol[2]. The usage of the BAND-AiDe tool is demonstrated through safety and sustainability verifications for: i) a *single medical device*, and ii) a *network of worker nodes*, as summarized in Figure 12 and described in the following subsections.

5.1 Safety and Sustainability Verification of a Single Wearable Medical Device

This subsection presents the safety and sustainability verification for a single high-power wearable medical device. To this effect, the medical device considered is a TelosB mote interfaced with a Smith fingertip pulse oximeter (PPG) device (`http://www.smithsoem.com/`) deployed on the index finger. The pulse oximeter probe which is in direct contact with the human finger passes light at a particular intensity through the finger during its operation. The pulse rates are then derived from the

[2]The threshold indicated in the figure is specific to the peak detection [Banerjee et al.] process and is not the same as the requirements thresholds discussed in this paper

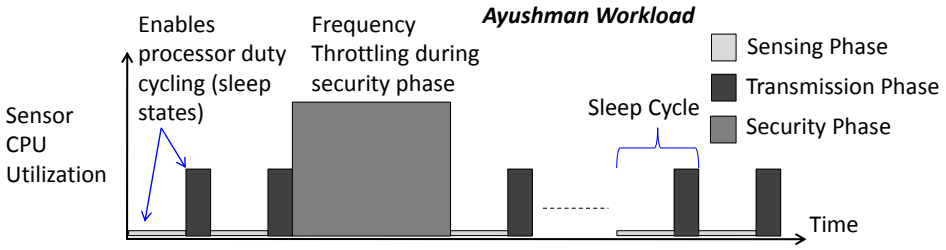

Fig. 10. **Ayushman workload showing duty cycling opportunities and variation in processing requirements. The processing requirements reflect power consumption trends during the application execution. Higher bars indicate higher processor utilization as well as higher power consumption.**

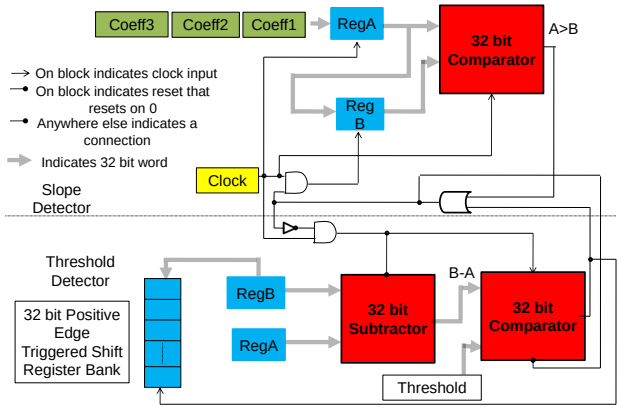

Fig. 11. Implementation logic for Peak Detection

modulations in the sensed light intensity. Power is consumed by the device to execute the Ayushman workload, i.e. sensing, transmission, and PKA execution, as shown in Figure 10.

5.1.1 *BAND-AiDe Inputs.* The safety requirement input to BAND-AiDe is the upper threshold on the skin temperature, which is 39 °C as obtained from the Henriques Moritz equation [Henriques and Moritz 1947]. For sustainability, the requirement is to keep the power consumption of the device lower than the available power from the scavenging sources. Pennes' bio-heat equation is used to characterize the thermo-dynamic processes. The thermo-dynamics of the finger comprises of heat transfer mechanisms such as thermal conduction, convection, radiation, and electro-magnetic absorption. The thermal safety analysis parameters include the time steps and space granularity (e.g. grid size, where a grid is the smallest volume of the human body within which the temperature is assumed to be constant) of the solvers for equations (in this case, the Pennes' equation) describing the thermo-dynamic processes.

Verification	Input	Model	Analysis
Safety and sustainability of a single wearable medical device (Pulse Oximeter)	**Requirements** : *Safety:* Threshold Temperature T_{th} of the human body which should not be exceeded [Henriques and R. 1947]. *Sustainability:* Device power consumption less than available power from scavenging sources. **BAN system**: Single worker node consisting of a TelosB mote interfaced with the fingertip Pulse Oximeter device deployed on the index finger. Scavenging sources are considered on the human body which charge the nodes through inductive charge transfer. **Analysis Parameter :** Differential equation solver FDTD parameters, (time step and space steps)	**Requirements Model** Requirement Verification Parameter T_{th} **BAN Model** **GCPS** - 1 **LCPS**. **LCPS - Computing Unit (CU) + ROIm** **CU –** subcomponents + properties subcomponents – LED, Radio, Processor, Scavenging source properties – Power dissipation, Temperature **ROIm** – Physical Property + Physical Dynamics + Region Boundary Physical Property – Temperature Physical Dynamics – Penne's bio heat equation Region Boundary – 30 mm by 30 mm square region **ROIn –** Charging range of the scavenging source **Analysis Parameter** Time Step and Space granularity parameters of FDTD solver	**Safety:** Thermal map of the fingertip skin for continuous operation of the pulse oximeter is tested against safety threshold set by the requirements. **Sustainability:** The power consumption of the device is compared against the available power from scavenging sources.
Safety evaluation of Network of Devices communicating securely	**Requirements** : *Safety:* Lower bound on the tissue temperature for the optimal cluster head selection sequence. *Sustainability:* Budget on the available power from the energy scavenging sources. **BAN system**: Network of worker nodes implanted within the human tissue. The worker nodes are interfaced with EKG sensors. Communication protocol is cluster based [Heinzelman et al 2000], where several nodes form a cluster with a nominated cluster head. The cluster head collects data from all the cluster members and sends them to the wearable worker node. A cluster head selection sequence is specified, which denotes the order in which cluster heads are selected during the data transfer process. The Ayushman health monitoring application is executed on each node. The radio of each worker node can be turned off during different stages of their operation. Scavenging sources charging the nodes via inductive charge transfer are assumed. **Analysis Parameter :** Cluster head selection sequence, differential equation solver FDTD parameters, (time step and space steps) Sensing Rate, data transmission rate, rate of PKA execution, time interval of observation.	**Requirements Model** Upper threshold T_{th} on the maximum temperature rise of the human tissue **BAN Model** **GCPS – n LCPS** **LCPS – Computing Unit (CU) + ROIn + ROIm** **CU –**properties properties – Power Dissipation **ROIn –** Monitored Property + Region Boundary Monitored Property – Radio signal strength Region Boundary – Communication Range (intersection of ROIn indicate connectivity) **ROIm –** Physical Property + Physical Dynamics + Region Boundary Physical Property – Temperature Physical Dynamics – Penne's Equation Region Boundary – preset value (intersection of ROIm require evaluation of cumulative effect) **LCPS – Scavenging Source + ROIn** **CU –** properties properties - Available power for scavenging source **ROIn –** A worker node receives power from a scavenging source if it falls inside the ROIn. **Analysis Parameter** Cluster head selection sequence Time Step and Space granularity parameters of FDTD solver Data transmission time t_{TX} , Sensing time t_s and PKA execution time t_{PKA}	**Safety:** Each cluster head selection sequence is evaluated to compute the thermal map of the tissue. Different cluster head selection sequences are compared based on the maximum temperature in the control volume. **Sustainability:** 24 hr operation of the Ayushman application was considered where sensing was performed at a rate of 60 samples per seconds, data communication every 5 seconds and PKA operation onde in 24 hrs

Fig. 12. BAND-AiDe usage for safety and sustainability evaluations

5.1.2 *BAND-AiDe Model.* The requirement and analysis parameter modeling involves representation of the skin temperature threshold, available power from the scavenging sources, the scavenging duration, and the time steps and grid sizes (to solve Pennes' equation) as constants. For the BAN-CPS modeling, the GCPS is represented as a system with a single LCPS. The medical device is modeled as the computing unit, which has several subcomponents such as LED array, radio, and processor. These subcomponents are the generic components of the pulse oximeter device. Each subcomponent has a set of physical properties (such as power dissipation, operating temperature) that model their thermal characteristics. The ROIm models the thermodynamics of the human skin using the Pennes' bioheat equation as follows:

$$\rho C_p \frac{dT}{dt} = K \bigtriangledown^2 T - b(T - T_b) + \rho \mathrm{SAR} + P_c + A \times \sigma(T_r^4 - T^4), \quad (1)$$

where ρ is the mass density, C_p is the specific heat, K is the thermal conductance, T is the temperature of the skin, P_c is the power generated by any heat source (i.e.

Table II. Skin temperatures after eight hours of pulse oximeter operation at different device temperatures (Burn threshold 39 °C)

Device Temperature	Maximum Skin Temperature
43.0 °C	38.2 °C
43.5 °C	38.5 °C
44.0 °C	39.2 °C
44.5 °C	39.4 °C
45.0 °C	39.7 °C

the device), A is the surface area of the radiating entity (i.e. the LED array in case of the pulse-oximeter), T_r is the surface temperature of the radiating entity, b is the blood perfusion constant, T_b is the blood temperature, and SAR is the specific absorption rate of the skin (i.e. the amount of electromagnetic radiation absorbed by unit volume of the skin).

The region boundary of the ROIn is preset to a 30mm × 30mm square region on the fingertip skin, which is the size of the pulse-oximeter probe (`http://www.smithsoem.com/`) that is in direct contact with the fingertip. The ROIn also models the range, up to which a scavenging source can charge a sensor node. To this effect, only body heat and sunlight are considered as the possible scavenging sources at the fingertip. The operating temperature of the pulse-oximeter probe is assumed to be constant [Greenhalgh et al. 2004]. This is because the Ayushman workload (Figure 10) is highly repetitive, which causes the probe temperature to reach a steady state quickly. Detailed BAND-AiDe implementation is shown in Appendix A.3. Given the inputs and the BAND-AiDe model, the BAND-AiDe analyzer performs the safety and sustainability analysis (described in Sections 5.1.3 and 5.1.4, respectively) based on the work-flow in Figures 4 and 8.

5.1.3 *Safety Verification.* BAND-AiDe analyzer computes the temperature at different points on the skin by solving the Pennes' equation using the FDTD approach. Table II shows the maximum skin temperature reached during the eight hours of operation of the pulse oximeter at different device temperatures. A sample thermal map of the skin for a pulse oximeter operating temperature of 44 °C is shown in Figure 13. It can be verified that the maximum temperature reached after eight hours of operation is 39.2 °C, which violates the thermal safety requirement. An experimental study performed on pulse oximeter thermal safety [Greenhalgh et al. 2004] shows that blisters are observed in human skin when a pulse oximeter is operated continuously for eight hours at a device temperature of 44 °C. Our results concur with these experimental observations and are hence verified.

5.1.4 *Sustainability Verification.* For sustainability analysis, the BAND-AiDe analyzer first extracts the power consumption characteristics of the sensor node from the model. The power consumption of the PPG sensor is 60 mW (`http://www.nonin.com/documents/OEM_Family_Brochure.pdf`) while the sensor node incurs another 60 mW of power because of execution of the Ayushman application. The power consumption of sensor node was obtained from experimental measurements on the TelosB platform. The total power consumption of the worker node is then 120 mW which is easily sustainable through a combination of body heat and sunlight (Table I). We do not need to consider any duty cycling of the sensor node

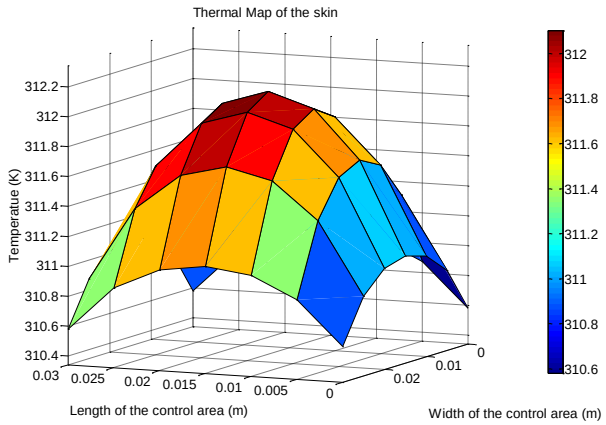

Fig. 13. Thermal map of fingertip skin for 8 hrs of pulse oximeter operation at 44 °C temperature

since it is already sustainable. Further, since body heat and sunlight offer lower power compared to the other scavenging sources (Table I), sustainability with these two sources would mean the other sources can also sustain the device operations.

5.2 Safety and Sustainability Verification of Network of Devices

This section presents the safety and sustainability verification for a network of worker nodes. To this effect, we consider low-power devices (as worker nodes), e.g. EKG sensors, interfaced with the TelosB motes. High power nodes are not considered since it has already been verified (in Section 5.1) that even a single such node can cause safety violations. Cluster based multi-hop communication protocol is used [Heinzelman et al.] for the network. In this protocol, the worker nodes in the BAN form a cluster. Nodes in a cluster nominate a leader node, a.k.a. the cluster head. All the non-leader nodes transmit their sensed data to the cluster head. The cluster head then forwards these data to the base station, and hence has a considerably high communication workload. The absorption of electromagnetic radiation (because of communication) can cause heat dissipation, which in turn may lead to significant thermal effects in the surrounding human tissue [Tang et al. 2005]. Periodic changes in the cluster head are required to reduce the maximum tissue temperature during the communication operation.

5.2.1 *BAND-AiDe Inputs.* Similar to the single device verification in Section 5.1, the safety requirement input for verifying the network of nodes is the upper threshold on the skin temperature, i.e. 39 °C. For sustainability verification, the available power from the scavenging sources and the parameters of the Ayushman application are provided as input to the BAND-AiDe framework. The exact values use for the analysis are shown in the Tables I and III. Analysis parameters corresponding to the Pennes' equation are same as that in Section 5.1. The control volume was divided into 30 × 30 cells where the cell size was set to 0.005m. The aggregation function for the heat effect from multiple contributing nodes is provided as follows: i) summation of the SAR values from the contributing nodes; ii) summation of the power generated from the contributing nodes; and iii) apply the summed SAR and

Table III. Parameter Values

Parameter	Value	Methodology
t_s	5 s	Ayushman workload characteristics
t_{Tx}	0.39 s	Time taken to transfer five seconds of 32 bit data values sampled at a rate of 60 per second. Transfer rate is 24 Kbps which is standard for Chipcon radio [Venkatasubramanian et al. a]
t_{PKA}	16.36 s	Measured time in TelosB motes [Venkatasubramanian et al. a]
P_{radio}	56 mW	Measurements from the Chipcon radio in TelosB motes [Venkatasubramanian et al. a]
P_{PKA}	3 mW	Measured power of the TelosB mote while executing PKA [Venkatasubramanian et al. a]
P_{proc}	0.01 mW	Idle power of the TelosB mote [Venkatasubramanian et al. a]

generated power values in the Pennes' equation (i.e. Equation 1). In addition, the leadership sequence is input as an analysis parameter.

5.2.2 *BAND-AiDe Model.* GCPS consists of multiple LCPSs. The LCPS modeling for each worker node is same as in Section 5.1. In addition, the ROIn of each LCPS models the communication range of the node. The intersections between the ROIns reflect the connectivity among the corresponding worker nodes. The leadership sequence is represented as a string of constant integers. Detailed BAND-AiDe implementation is shown in Appendix A.4. Scavenging nodes are further modeled as LCPSs, where the ROIn represents the inductive charging range. Intersection of the ROIn of a worker node and a scavenging source means that the worker node can extract power from that source. The energy consumption of the BAN during execution of Ayushman is modeled as follows:

$$\text{Total BAN Energy} = \text{Sensing Energy} + \text{Data Transmission Energy} + \text{PKA computation energy}$$
$$\Rightarrow E_{BAN} = nxt_s(P_{proc}) + nxt_{Tx}(P_{radio} + P_{proc}) + t_{PKA}(P_{PKA} + P_{radio})(\tfrac{n(n-1)}{2}), \quad (2)$$

where E_{BAN} is the total energy of the BAN, n is the total number of nodes in the BAN and x is the number of sleep cycles. The power consumption profile of the BAN is clearly depicted in Equation 2. In the sensing phase, when the radio is off, a worker node consumes t_sP_{proc} amount of energy. In the transmission phase, both the processor and the radio are on and the net energy consumption is $t_{Tx}(P_{radio}+P_{proc})$. Each of the n nodes spend $(t_s)P_{proc}+t_{Tx}(P_{radio}+P_{proc})$ amount of energy during one sleep cycle (there are x number of sleep cycles for each node). Further, once a day the nodes should perform pair-wise PKA execution to ensure the freshness of the communication security key. This requires $\frac{n(n-1)}{2}$ number of PKA execution, each of them taking t_{PKA} amount of time and consuming P_{PKA} amount of power. The number (x) of sleep cycles in a day can be computed from the timing information of the different stages of Ayushman, as given below:

$$\text{Sensing time} + \text{transmission time} + \text{PKA execution time} = 1 \text{ day}$$
$$\Rightarrow (t_sx) + (t_{Tx})nx + t_{PKA}\tfrac{n(n-1)}{2} = 24 \times 3600. \quad (3)$$

Here we consider that all the nodes sense at the same time and data communication is performed in a Time Division Multiple Access (TDMA) fashion; hence requiring n transmissions per sleep cycle. Detailed BAND-AiDe implementation is presented

Table IV. Tissue temperature rise for different leadership sequences (Burn threshold 39 °C)

Leadership Sequence	Maximum Tissue Temperature	
	1000 Sec Exposure	2 Days Exposure
(5 2 8 6 1 7 3 4 10 9)	37.1145 °C	37.1632 °C
(5 7 4 1 6 10 8 2 9 3)	37.1130 °C	37.1614 °C
(1 6 9 10 2 7 5 4 3 8)	37.1124 °C	37.1757 °C
(5 7 1 9 10 8 4 2 6 3)	37.1130 °C	37.1585 °C

in Appendix A.5.

5.2.3 *Safety Verification.* To evaluate the tissue temperature distribution, Pennes' bio-heat equation is solved using the FDTD solvers (as in Section 5.1.3). This aggregate effect was calculated by summing up the heat contribution of each node to a particular grid, as indicated in Section 5.2.1. The power consumption of leader worker node executing the Ayushman application was 60mW [Venkatasubramanian et al. a] while that of a non leader worker node was 12 mW. This power consumption was experimentally measured for TelosB motes at 0 dB and -7 dB radio attenuation, respectively. For a sample BAN cluster of 10 worker nodes, the leaders were changed every second. Each leadership sequence was operated once for a short period of 1000 seconds and then for a long duration of two days. Our results for 1000 second of exposure matches with the observations in [Tang et al. 2005]. Table IV shows maximum tissue temperatures for different leadership sequences at different exposure times. The maximum temperature is below the safety threshold of 39 °C for all these cases. It can be seen from the table that for a short duration of exposure, different leadership sequence does not have much effect on the tissue temperature rise. However, for longer durations, the temperature rise is significant (around 0.02 °C). This shows that for long term operation of implanted network of medical devices the leadership sequence plays an important role in thermal safety.

5.2.4 *Sustainability Verification.* For sustainability verification, we consider the power consumption of the BAN in each phase of Ayushman. During the PKA execution, which happens only once in a day the scavenging sources have to supply P_{PKA} amount of power to each of the participating worker node for $\frac{n(n-1)}{2}$ times. The rest of the energy stored in the scavenging sources should sustain the operation of the worker nodes for the rest of the day (i.e. provide enough energy to sustain x number of wake up cycles). During the data transmission and sensing phase of Ayushman, $P_{radio} + P_{proc}$ and P_{proc} amount of power has to be supplied to the worker nodes, respectively. The number of wake up cycles, x_{sca}, that the scavenging source can sustain is determined from Equation 4.

$$x_{sca} = \frac{E_{TotSca} - (P_{PKA} + P_{radio})t_{PKA}\frac{n(n-1)}{2}}{(t_s P_{proc} + t_{Tx}(P_{radio} + P_{proc}))n} \tag{4}$$

If $x_{sca} > x$, then we conclude that the scavenging source can sustain the operation of the BAN throughout the day (line 7). We consider combination of scavenging techniques to determine the maximum number of worker nodes that they can sustain in a day. Table V gives the number of worker nodes sustained by different combination of scavenging sources for a period of 24 hours of continuous operation. It shows two cases of operation—with and without duty cycling. Significant dif-

Table V. Energy Scavenging Results

Combination of Scavenging Sources	Number of nodes sustained with duty cycling	Number of nodes sustained without duty cycling
All four	217	9
Body Heat + Ambulation	177	9
Respiration + Ambulation	162	5
Body Heat + Respiration	145	5
Ambulation + Sunlight	131	2

ference in number of sustained nodes is observed and duty cycling is advised for better sustainability of the BAN.

Given the modeling and analysis methodology in the case study, it can be observed that a substantial part of the model—e.g. the power models of the nodes, the node deployment model, the node duty cycling strategy, the model of the human body, and the model for the Ayushman workload—can be reused for both safety and sustainability analysis. In addition, safety analysis requires the specification of heat transfer equations while the sustainability analysis requires the power models of the scavenging sources. Model re-usability can potentially expedite the requirement verification process.

6. DISCUSSION

The previous section showed how BAND-AiDe can be used to perform safety and sustainability analysis of BANs. In this regard thermal safety of BANs and sustainability to secure inter-device communication were considered. This section further discusses the applicability of BAND-AiDe in other scenarios where safety and sustainability can be important. The ability to specify two way interaction between the ROIn and the ROIm in BAN-CPS is of special interest in this discussion.

Physical processes in the ROIm can affect the monitored parameters in the ROIn. Consider the example where an implanted worker node that measures physiological values from the human body and transfers it to a the base station. Let the ROIn be defined as the communication range of the worker node and the ROIm be defined as the area of the surrounding tissue that receives thermal energy from the sensor due to its heat dissipation. Implantation often leads to growth of tissue around the computing unit resulting in a change in the ROIm of the system [Paul et al. 2007]. However, this phenomenon leads to a change in the electromagnetic environment of the worker node thus altering its communication capabilities or affecting the ROIn. The designer of the BAN can then perform an analysis on the effect of tissue growth on the communication range of the worker node and plan its deployment accordingly (place the worker nodes in areas with low tissue growth rate).

The operations in the ROIn may also affect the ROIm parameters in a BAN. Consider the example of an implanted cluster of worker nodes, each of them connected to a base station through wireless links. The monitored parameter in the ROIn is the connectivity of the worker nodes while the ROIm is the the region of the tissue that gets heated due to communication workloads in the worker nodes. Connectivity in this scenario is the ability of all nodes in the cluster to communicate with the base station. There can be two choices to achieve connectivity in this cluster: 1) each worker node has an one hop connection to the base station and 2) worker nodes are

connected to the base station through a multi-hop connection. It is often possible to reduce communication range of worker nodes and still maintain connectivity in case of the second alternative. A reduction in communication range (ROIn) also reduces the power consumption of the worker nodes hence favorably affecting the ROIm. Thus the designer can evaluate multi-hop or one-hop design decisions based on analysis performed using the BAN-CPS model.

Further, in case of multiple BANs, such as in a conference room with a group of people, each having a single BAN on them, it is possible that the operations in one BAN can affect that of the other [Natarajan et al.]. The BAN-CPS model can however capture such a case by changing the control volume for the GCPS from the body of one human to the group of humans close to each other. A single device can have impact on multiple human bodies. The physical dynamics in the corresponding ROIms may depend on the corresponding human body. These scenarios are complex and have not been modeled till date. However, the proposed abstract model of a BAN gives insight to model and analyze such complex situations. Further, mobility among BANs can cause complex interaction patterns, which can also be stochastic in nature. We plan to consider such scenarios in future versions of BAND-AiDe.

7. CONCLUSIONS

This paper proposed a tool, BAND-AiDe, that enables BAN designers to develop cyber-physical oriented analysis driven abstract models of BANs and perform evaluation of the model for the *safety* and *sustainability* requirements. The tool compliments the existing tools to perform analysis against the design requirements of accuracy, minimal resource usage and low latency. To this effect, a generic CPS model of BANs (BAN-CPS) was developed where dedicated constructs that model intentional and un-intentional interactions of BANs with the human body were provided. The implementation of the tool uses industry standard model specification language AADL and incorporates the new constructs for BAN-CPS as an annex. It is contended that the CPS model is generic enough to analyze a varied set of BAN applications for the safety and sustainability requirements. Through a case study involving wearable and implanted sensors nodes, the usage of BAND-AiDe has been demonstrated. The case study depicts re-usability of BAND-AiDe models, which is a useful feature to expedite the requirement verification process.

Acknowledgments

This research was funded in part by National Science Foundation grant CNS-0831544. We are also thankful to Dr. Krishna Kumar Venkatasubramanian for providing useful insights.

REFERENCES

Banerjee, A., Venkatasubramanian, K., and Gupta, S. Challenges of implementing cyber-physical security solutions in body area networks. In *Procs. of Intl. Conf. BodyNets '09.*

Chen, W., Sonntag, C., Boesten, F., Bambang Oetomo, S., and Feijs, L. 2008. A power supply design of body sensor networks for health monitoring of neonates. In *Intl. Conf. on Intelligent Sensors, Sensor Networks and Information Processing,*. 255 –260.

Elena, G.-M. and José, M. 2006. Argospe: Model-based software performance engineering. In *ICATPN*. 401–410.

Greenhalgh, D. G. M., Lawless, M. B. R., Chew, B. B., Crone, W. A., Fein, M. E., and Palmieri, T. L. M. 2004. Temperature threshold for burn injury: An oximeter safety study. *Journal of Burn Care and Rehabilitation 25,* 5, 411–415.

Gyselinckx, B., Van Hoof, C., Ryckaert, J., Yazicioglu, R., Fiorini, P., and Leonov, V. Human++: autonomous wireless sensors for body area networks. In *Procs. of IEEE Custom Integrated Circuits Conference, 2005.* 13 – 19.

Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In *Procs. of IEEE HICSS '00-Volume 8*. Washington, DC, USA, 8020.

Henriques, F. C. J. and Moritz, A. R. 1947. Studies of thermal injury: I. the conduction of heat to and through skin and the temperatures attained therein. a theoretical and an experimental investigation. In *Am J Pathol.* 530–549.

Karsai, G. and Sztipanovits, J. Model-integrated development of cyber-physical systems. In *Procs. of Intl. workshop SEUS '08*. Springer-Verlag, Berlin, Heidelberg, 46–54.

Korhonen, I., Parkka, J., and Van Gils, M. 2003. Health monitoring in the home of the future. *Engineering in Medicine and Biology Magazine, IEEE 22,* 3 (May-June), 66–73.

Milenković, A., Otto, C., and Jovanov, E. 2006. Wireless sensor networks for personal health monitoring: Issues and an implementation. *Computer Communications (Special issue: Wireless Sensor Networks: Performance, Reliability, Security, and Beyond 29*, 2521–2533.

Mistry, P., Maes, P., and Chang, L. Wuw - wear ur world: a wearable gestural interface. In *CHI EA '09: Procs. of Intl. Conf. on extended abstracts on Human factors in computing systems*. ACM, New York, NY, USA, 4111–4116.

Natarajan, A., de Silva, B., Yap, K.-K., and Motani, M. To hop or not to hop: Network architecture for body sensor networks. In *Procs. of SECON '09.* 1–9.

Paradiso, J. A. and Starner, T. 2005. Energy scavenging for mobile and wireless electronics. *Pervasive Computing, IEEE 4,* 1 (Jan.-March), 18–27.

Paradiso, R., Loriga, G., and Taccini, N. 2005. A wearable health care system based on knitted integrated sensors. *IEEE TITB 9*, 337–344.

Park, G., Rosing, T., Todd, M. D., Farrar, C. R., and Hodgkiss, W. 2008. Energy harvesting for structural health monitoring sensor networks. *Journal of Infrastructure Systems 14*, 64–79.

Paul, D., Nathan, L., Bazhang, Y., Yvonne, M., and Moussy, F. 2007. Study of the effects of tissue reactions on the function of implanted glucose sensors. *Journal of Biomedical Materials Research Part A*, 699–706.

Pennes, H. H. 1948. Analysis of tissue and arterial blood temperature in the resting human forearm. In *Journal of Applied Physiology.* Vol. 1.1. 93–122.

Prasad, V., Yan, T., Jayachandran, P., Li, Z., Son, S., Stankovic, J., Hansson, J., and Abdelzaher, T. Andes: An analysis-based design tool for wireless sensor networks. In *Procs. of RTSS 2007.* 203–213.

Sandeep, K.S. Gupta. 2009. A Tool for Designing High-Confidence Implantable BioSensor Networks for Medical Monitoring. *Joint Workshop On High Confidence Medical Devices, Software, and Systems (HCMDSS) and Medical Device Plug-and-Play (MD PnP) Interoperability*, .

Schwiebert, L., Gupta, S. K., and Weinmann, J. Research challenges in wireless networks of biomedical sensors. In *Procs. of MobiCom '01.* ACM, New York, NY, USA, 151–165.

Tang, Q., Tummala, N., Gupta, S., and Schwiebert, L. 2005. Communication scheduling to minimize thermal effects of implanted biosensor networks in homogeneous tissue. *IEEE Transactions on Biomedical Engineering, 52,* 7 (July), 1285–1294.

Tuinenga, P. W. 1991. *Spice: A Guide to Circuit Simulation and Analysis Using PSpice.* Prentice Hall PTR, Upper Saddle River, NJ, USA.

Venkatasubramanian, K. K., Banerjee, A., and Gupta, S. K. S. Green and sustainable cyber-physical security solutions for body area networks. In *Procs. of IEEE BSN '09.* Washington, DC, USA, 240–245.

Venkatasubramanian, K. K., Banerjee, A., and Gupta, S. K. S. Plethysmogram-based secure inter-sensor communication in body area networks. *IEEE MILCOM 2008*, 1–7.

Venkatasubramanian et. al. 2005. Ayushman: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed. In *Distributed Computing in Sensor Systems.* 406–407.

Weininger, S., Pfefer, J., and Chang, I. Factors to consider in a risk analysis for safe surface temperature. In *IEEE Symposium on Product Safety Engineering, 2005.* 83–91.

A. APPENDIX

A.1 AADL modeling

In this section a short introduction to the AADL specific constructs used in the paper is provided. AADL model specification is inherently hierarchical in nature where the user develops a system as a congregation of components. Such a composite model is declared by the **system** keyword in AADL. Each system has two parts to its specification as shown in the Figure 14:

(1) System Declaration - It is the definition of the component that includes its inputs and outputs through which other components can communicate with it denoted by the keyword **features**, salient properties of the component that characterizes its behavior in the particular analysis denoted by the keyword **properties** and any functionality that the user wants to include which is not supported by AADL denoted by the keyword **annex**. AADL has the provision for developing annexes where an user can implement customized specification rules and constructs to supplement the AADL specification language.

(2) Component Implementation denoted by the keyword **implementation** - This is a specific instance of the declaration. In this part of the specification the subcomponents of the component are specified. The different subcomponents are interconnected through specific connection definitions denoted by the keyword **connections** in the desired manner to setup the model of the component. Specific values to the properties and annex variables of the component are assigned.

```
system Component
  features
  INPUT: input type;
  OUTPUT: output type;
properties
  P1: property type;
end Component;

system implementation Component.imp
  subcomponents
  C1: component type;
  C2: component type;
properties
  P1: specific implementation;
annex
  A1: specific implementation;
connections
  connection between inputs and outputs of two subcomponents: connection type;
end Component.imp;
```

Fig. 14. Component Declaration and Implementation

A.2 Physical Dynamics Modeling in AADL

Physical dynamics are generally determined following certain form of equations which are often very complex differential equations. AADL framework does not

have any means to specify equations in the model. In this regard an annex (BAN-CPS Annex) was developed that provides generic constructs to specify equations in the AADL model.

The BAN-CPS Annex supports two types of equations: 1) Representing boundary conditions; and 2) Differential and algebraic equations representing physical process. *States* construct represent different modes a component can be in. In our model we are consider only one mode. Thus, 'So' is both initial and final mode. *Transitions* construct represent event based mode transitions. Since we are not using any external event we do not have any transition.

Boundary_condition: Represents a keyword indicating what follows is a boundary condition Physical Process Equation: For the purpose of illustration we are considering a partial differential equation $PDer1TIt := 0$. Tokens starting with $PDer$ indicate that the corresponding token represents a partial derivative. In the illustrative equation, the 1 (after $PDer$) indicates first order derivative; T is the dependent variable, and I indicates what follows is an independent variable. The interpretation of the illustrative equation is that the rate of change of temperature w.r.t time is 0.

```
Annex behavior_specification
{**
States
S0: initial complete state;
Transitions
So-[] s0 {

Boundary_condition :=  radius * radius;

%physical process equation
PDerTIt := 0;

};
**}
```

A.3 AADL Implementation for Safety and Sustainability Verification for Single Node

A sample code for the AADL implementation of the analysis technique is shown in Figure 15. In this analysis there is only one LCPS. The LCPS consists of the computing unit (pulse oximeter) and the ROIm. The ROIn is not required to be modeled as we are only considering the unintended effects of the computing system on the physical environment. The model of the computing unit is derived from the generic pulse oximeter model proposed by TI ($http://focus.ti.com/docs/solution/folders/print/330.html$). It consists of several subcomponents only a few important ones are shown in the Figure 15. The computing system consists of an LED array (the pulse oximeter probe), a photo detector (pulse oximeter sensor), a processor, a radio and a system bus that connects these components. Each of the subcomponents of the computing system has two types of properties, **ComputationalPropertySet** and **PhysicalPropertySet**, which characterizes the computing and the physical behavior of them. For example, the Radio subcomponent

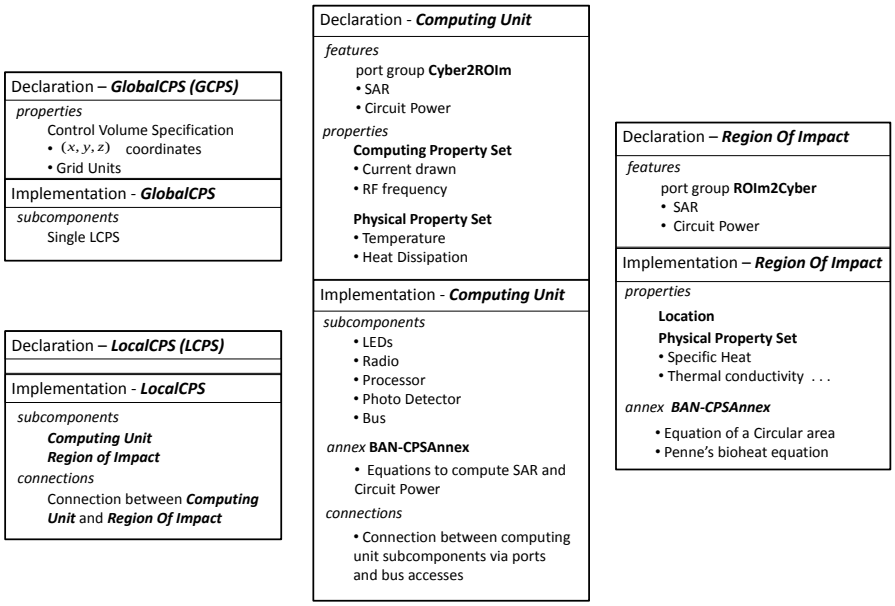

Fig. 15. AADL code structure for Pulse Oximeter Safety modeling

has properties like current drawn and the frequency of operation which specifies its communication properties. Further, it has properties such as heat dissipation which characterizes its physical (thermal) behavior.

In case of the pulse oximeter, the LED array (probe) is main contributor to the heat energy transferred to the human finger (ISO 9919 standard). It is required to test the operation of the system for thermal safety at different temperatures of the pulse oximeter probe. Thus the LED subcomponent of the computing system has a temperature property which can be varied in different experiments. The ROIm requires the specification of two parameters: 1) the region boundary, which is assumed to be circular for this particular analysis and 2) the equation characterizing the physical behavior in the ROIm, which is the Pennes' bio-heat equation. Specification of both the parameters are achieved using the BAN-CPS Annex, that allows representation of equations in AADL models. This annex was developed to include dedicated constructs for specifying complex differential equations. The interaction between the computing unit and the ROIm is through energy transfer via heat and electromagnetic radiation. Thus the port group **ROIm2Cyber** has data ports named SAR and Circuit Power which represent the energy transfer due to electromagnetic absorption and computing unit power dissipation respectively.

A.4 AADL Implementation for Safety Verification of Network of Nodes

In this analysis, multiple worker nodes in the BAN are involved hence the modeling of a network of sensors is required. The computing unit (as shown in Figure 16) is modeled as a system of two subcomponents: 1) a heat dissipation unit (PowerCircuitry), and 2) a source of electromagnetic energy (SAR). The LCPS (Figure 16)

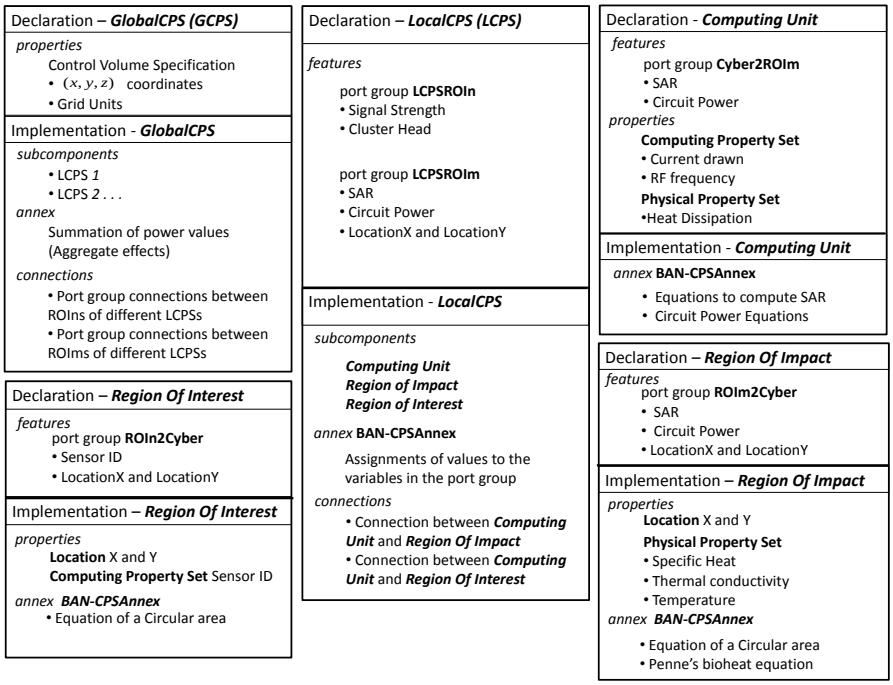

Fig. 16. AADL code structure for Multi-hop-communication evaluation

consists of the computing system and the ROIm and ROIn. The ROIm is the same as the previous analysis, however it has an extra parameter that specifies its location with respect to the grid defined in the GCPS. This location parameter along with the boundary equation of the ROIm enables the analysis plug-in to determine possible overlap (global interactions) between ROIms. Moreover, in this evaluation the communication range of each worker node needs to modeled in order to represent cluster formation. This is done by specifying ROIn for each worker node, where the boundary of the ROIn represents the communication range of each node. In this analysis the communication range for every node are assumed to be circular which is reflected in the annex equation for the ROIn. In the GCPS implementation each of the LCPS are connected via port group so as to facilitate global interactions among them (the existence of which is decided in the analysis plug-in). The aggregation equations for computing the heating effects in the regions where the ROIms overlap are specified using the BAN-CPS Annex in the GCPS as shown in Figure 16.

A.5 AADL Implementation for Suatainability Verification of Network of Nodes

The AADL implementation of the sustainability analysis involves the specification of three entities: 1) The power consumption model of the computing unit due to the privacy enhanced health monitoring application, 2) the power supply models of the scavenging techniques and 3) the duty cycle of operation of the computing units. The sample code for the implementation is shown in the Figure 17.

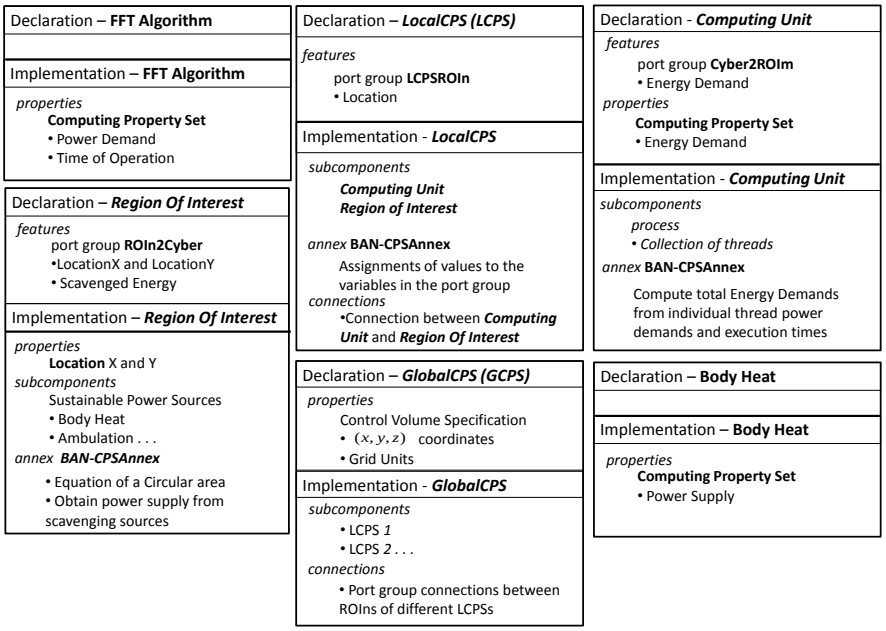

Fig. 17. Sustainability analysis AADL code sample

Sensing and DataTransmission steps are modeled as Threads ($Sensing_algorithm$ and $DataTranmsmission_algorithm$). These steps are characterized by properties: current consumption, execution time and the rate of execution. These properties are part of Computing Property Set. PKA protocol is modeled as a process ($Computing.Security_PkA$), all the 11 stages of this protocol are modeled as Threads.

A Sustainable Power source is modeled as a System (Power Source). Body Heat, Ambulation and Respiration are different types of power sources that we are considering in this analysis. These are modeled as implementations of Power Source. Voltage generated by these power sources are modeled by voltage property. Some of these stages consume different amounts of current when radio is turned on or off, these operating characteristics are represented as modes(RadioOn and RadioOff)in a thread.