Data-Centered Runtime Verification of Wireless Medical Cyber-Physical System

Yu Jiang, Houbing Song, Rui Wang, Ming Gu, Jiaguang Sun, and Lui Sha

***Abstract*—Wireless medical cyber-physical systems are widely adopted in the daily practices of medicine, where huge amounts of data are sampled by the wireless medical devices and sensors, and is passed to the decision support systems (DSSs). Many text-based guidelines have been encoded for work-flow simulation of DSS to automate health care based on those collected data. But for some complex and life-critical diseases, it is highly desirable to automatically rigorously verify some complex temporal properties encoded in those data, which brings new challenges to current simulation-based DSS with limited support of automatical formal verification and real-time data analysis. In this paper, we conduct the first study on applying runtime verification to cooperate with current DSS based on real-time data. Within the proposed technique, a user-friendly domain specific language, named DRTV, is designed to specify vital real-time data sampled by medical devices and temporal properties originated from clinical guidelines. Some interfaces are developed for data acquisition and communication. Then, for medical practice scenarios described in DRTV model, we will automatically generate event sequences and runtime property verifier automata. If a temporal property violates, real-time warnings will be produced by the formal verifier and passed to medical DSS. We have used DRTV to specify different kinds of medical care scenarios and have applied the proposed technique to assist existing wireless medical cyber-physical system. As presented in experiment results, in terms of warning detection, it outperforms the only use of DSS or human inspection, and improves the quality of clinical health care of hospital.**

***Index Terms*—Decision support system (DSS), real-time data, runtime verification, wireless medical cyber-physical system.**

I. Introduction

WITHIN the scope of cyber-physical-human medical system, clinical guidelines and decision support subsystems play a very important role in coordinating medical staffs to improve patient care. With interpreting text-based guidelines into some computer executable format, decision support systems (DSSs) are designed to monitor actions and observations during practice workflow, and generate reminders and advice when corresponding guideline is not satisfied. Lots of evidence have showed that, using clinical guideline-based DSS, quality of medical care sometimes even the survival rate of patients, would be improved, and the medical care practice variability would be reduced [22]. However, with rapid developments of medicine science and computer technology, pathological model of some disease are becoming more and more precise and complex, and more real-time vital signs about patient need to be sampled and analyzed to prevent some complex nondeterministic temporal potential complications, which brings new challenges to current simulation-based DSS.

For example, during the best practice guideline of ischemic stroke therapy [12], patient's neurological symptoms like speech difficulty and vital signs such as blood coagulation index should be monitored in real time, after the administration of recommended tissue plasminogen activator (rt-PA). If any of vital signs are out of range, stroke team will issue corresponding treatment orders to head nurse in ambulance or intensive care unit to prevent patient from life-threatening complications such as hemorrhagic bleeding. Timely response based on real-time data monitoring and runtime rigorous verification is highly desirable, because a huge number of brain cells die every second. Another example is about the best practice guideline of infants respiratory distress syndrome, vital signs about blood-gas values should be monitored. If it is continuously above the normal range for at least 3 h, the treatment is fine. But if it is too steep for at least 30 s, further emergency actions should be taken [5]. In both cases, specifying complex temporal properties for automatically rigorous verification would be more reliable than semiautomated manual vision inspection of current simulation-based DSS.

More specifically, through the discussion with physicians, we learned that those phenomenons bring new challenges to medical DSS in two aspects. First, although some guideline-based

Manuscript received March 3, 2016; revised May 8, 2016; accepted May 17, 2016. Date of publication May 27, 2016; date of current version August 1, 2017. This work was supported in part by the National Science Foundation (NSF) under Grant CNS 13-30077, Grant CNS 13-29886, and Grant CNS 15-45002, and in part by the National Science Foundation China (NSFC) under Grant 61303014. Paper no. TII-16-0255. *(Corresponding author: R. Wang.)*

Y. Jiang is with the School of Software, Tsinghua University, Beijing 100084, China, also with the Beijing Advanced Innovation Center for Imaging Technology, Capital Normal University, Beijing 100048, China, and also with the Department of Computer Science, University of Illinois at Urbana–Champaign, Champaign, IL 61820 USA (e-mail: jiangyu198964@126.com).

L. Sha is with the Department of Computer Science, University of Illinois at Urbana-Champaign, Champaign, IL 61820 USA.

H. Song is with the Department of Electrical and Computer Engineering, West Virginia University, Morgantown, WV 26506 USA.

M. Gu and J. Sun are with the School of Software, Tsinghua University, Beijing 100084, China.

R. Wang is with the College of Information Engineering, Beijing Advanced Innovation Center for Imaging Technology, Capital Normal University, Beijing 100048, China (e-mail: wangruicnu@126.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2016.2573762

DSS support static properties, runtime verification of complex temporal properties is not supported. Besides, not all vital signs will be stored in current patient record systems. Second, it not easy for medical staffs to monitor a huge number of vital signs for a long time, and input those conditions and violations into DSS in time. Statistics shows that medical staffs are under tremendous pressure and overloaded by a great amount of unorganized information. It is not easy to relate the information contained in the complex medical systems with temporal properties of complex complications with semiautomated manual vision inspection.

In practice, we propose a real-time data-based runtime verification technique to cooperate with current DSS, to release medical staffs from safety critical complex temporal properties and huge amounts of vital signs. It combines formal methods in software engineering and practice guidelines in medicine to rigorously verify runtime temporal properties automatically, and can be implemented and plugged in existing DSS to strength health care. A domain specific language DRTV is proposed to specify the medical care scenario, as well as data and properties contained in this scenario. The proposed language inherits some features from existing computer interpretable formations of guideline for compatibility, while focuses more on data part and enhances property specification ability with past time linear temporal logic [2]. Based on DRTV model, we develop a tool to automatically generate runtime monitors, which will continually extract scenario related data, parse their values to get event sequences, and input the event sequences to a runtime verification engine to rigorously check the temporal properties, accompanied with some interfaces for data communication. Overall, main contributions are as follows.

1) A verification technique based on real-time data of patient and runtime verification is adapted to cooperate with wireless medical cyber-physical system.
2) A domain specific language for specifying real-time data and complex temporal properties within a clinical scenario of best practice guideline are designed, and corresponding tools are implemented.
3) A real-device-based testing and evaluation are conducted to test the efficiency. To the best of our knowledge, this is the first study on applying runtime verification to improve the clinical health care.

II. Related Work

Last decades, health care organizations and providers pay many efforts to guideline application, that is, implementing well-validated and verified practice guidelines into computer-based DSSs to provide better health care [8]. Actually, according to the Institute of Medicine, these systems improve the acceptance of guideline with automation of medicine practice. Text-based guidelines are represented and encoded into a computer-interpretable format, such as Arden [7] and Asbru [5]. With the syntax and semantics of them, inference and decision making methodologies used in artificial intelligence such as rule-based reasoning, and probabilistic network can be designed and implemented. Then, DSSs such as Spock [24] and CREDO [6] are developed to monitor actions and observations of medicine staff and provide corresponding suggestions, through task execution, condition examination, and procedure visualization. However, many clinical problems are complicated and involving many timely decision-making according to a huge number of real-time vital signs. Then, task-based simulation and staff observation-based semiautomated collaboration of DSSs encounter major difficulties. Rather than semiautomated informal methods such as artificial intelligence algorithms, our work will use runtime verification engine to deal with real-time data automatically. In this way, real-time rigorously verified results will be produced to assist current DSSs.

For runtime verification, that is, verifying properties with runtime information of systems. It is effective to verify real-time temporal properties, and has been applied in many applications. Within last ten years, considerable amount of work has been invested in program runtime verification systems [4]. These pieces of work are often extensions of AspectJ [10] for java programs. For hardware runtime verification, property specification is usually translated into a hardware description such as Vhsic Hardware Description Language (VHDL) and Verilog, which is then synthesized into a netlist and loaded into dynamically reconfigurable blocks of field programmable gate array (FPGA) [16], [21]. Some work about the runtime verification of medical systems is presented in [9], [11], [13], and [14]. They focus on mitigating safety hazards of closed-loop or open-loop medical systems [1], [3]. They work on runtime safety and reliability status of the system devices, hardware and communications, and nothing is related to DSSs and clinical guidelines. For example, King *et al.* proposed a formal specification language to express and reason safety properties of on-demand medical systems [11]. Pajic *et al.* combined simulation-based analysis and model checking to guarantee the safety of closed-loop medical systems [20]. In [19], a model-driven approach allows us to prove safety properties of devices on the modeling level and ensures that the abstract models used in the verification process are sound with respect to actual dynamics of system. We conduct our work without considering the status of hardware systems, mainly focus on the real-time data of patient sampled in devices and their verification on temporal properties derived from clinical practice guidelines.

III. Verification Approach

In this section, we introduce how the workflow of real-time-data-based runtime verification technique cooperates with existing wireless medical cyber-physical systems, including domain specific language DRTV used to specify data and properties of medical care scenario, and semantics formalization to formalize the scenarios described in a DRTV model into the input sequence and automata for runtime verification.

A. Verification Workflow Overview

The proposed real-time-data-based runtime verification technique is presented in Fig. 1. First, we build a DRTV model to specify vital real-time data sampled by medical devices or from Electronic Patient Record, and temporal properties originated from clinical guidelines. For data part specification,

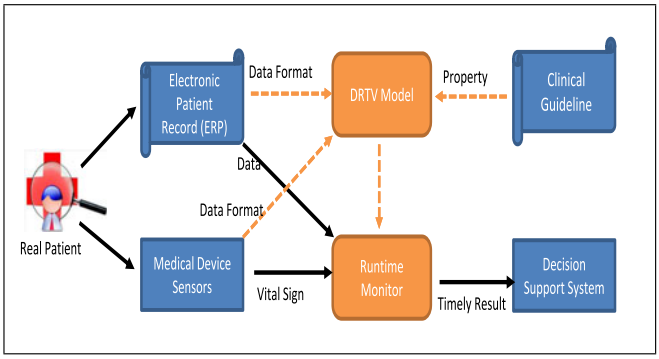


Fig. 1. Real-time-based runtime verification technique, and interfaces with main components in current medical care systems.

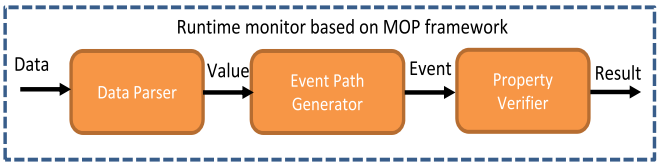


Fig. 2. Runtime monitor generated according to the DRTV model.

information such as data format, location, and type should be captured. For specification of property, $ptLTL$ formulae should be written correctly according to description of clinical guidelines. Also, event mapping expressions would be defined on current data, or historical data. Then, for medical practice scenario described in DRTV model, we will formalized it for automatical generation of corresponding runtime property monitor with a developed engine based on an Monitoring Oriented Programming (MOP) technique [17]. The automatically generated monitor will continually read real-time data or historical data, verify temporal properties on them, and produce output to assist DSSs to produce better health care.

1) Verifier: Then, let us see the structure of runtime monitor. As presented in Fig. 2, workflow of the generated runtime monitor by our developed engine is based on three components: data parser, event path generator, and property verifier. These three components are automatically derived from the DRTV model with some formalization rules implemented in the engine. They will cooperate together to accomplish the task that real-time patient data are processed to get runtime verification result, with main steps listed as follows.

1) *Data parser:* This component is formalized and automatically generated according to the data description part of DRTV model. With data parser, all relevant vital signs within model description will be abstracted from data packet sampled by medical devices, or from electronic patient records.
2) *Event path generator:* This component is formalized and automatically generated according to the event description part of DRTV model. With event parser generator, values of vital signs abstracted in previous step will be used to evaluate boolean formula to get corresponding events.
3) *Property verifier:* This component is formalized and automatically generated according to the property description part of the DRTV model. With property verifier, events generated in previous step will be read to decide the transition of monitor automata. If the automata transit to a violation state, timely response should be produced to the DSS to remind further actions of medical staffs. Otherwise, the monitor will continually read the event.

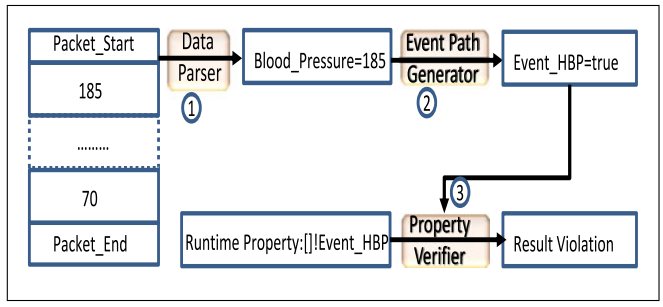


Fig. 3. Runtime verification example to monitor blood pressure.

An example of monitor workflow is presented in Fig. 3. Kernel of the real-time-data-based runtime verification technique is the DRTV model, which is independent of the format of existing computer interpretable guidelines. Besides, the automatically generated runtime monitor through a developed engine based on MOP is running independently from current DSSs. So, the proposed technique is platform independent, and could be customized and plugged into many existing medical care systems.

B. Domain Specific Language DRTV

The proposed domain specific language DRTV should provide the ability to describe data, event, and temporal properties in different medical scenarios, based on which, we will formalize those elements to generate runtime monitor. The language should also be clear to use. We survey many formats of existing computer interpretable guidelines, and build our syntax on them, with more focus on data and *ptLTL* formula property specification. For example, the data specification part in DRTV makes use of some features from syntax of Arden, a widely used clinical guideline modeling language. In this way, medical staffs and engineers of medical systems will be more familiar to understand and construct a DRTV model, even when they have little experience in runtime modeling or verification. Kernel syntax of the domain specific language DRTV is presented as folllows.

1) Scenario Module: Each DRTV model contains one module for a medical scenario. Each module starts with a reserved word *Scenario*, followed by scenario name and entity. The main entity consists of five constructs *data_resource, current_data, history_data, event,* and *property*. The first construct $data\_resource$ specifies resource of real time data. If the resource is medical device sensors, name and data packet length of the device need to be captured by construct $device\_name$ and $packet\_length$. If the resource is electronic patient record, name and record length of the patient record need to be captured by construct $record\_name$ and $record\_length$. The length will be used to help to locate and abstract data from data packet or patient record. Note that different medical device sensors

and electronic patient record systems will use different kinds of information format for transmission.

$$
\begin{aligned}
DRTV\_model ::= {} & 'Scenario' < module\_name > \\
& < module\_entity > \\
module\_entity ::= {} & < data\_resource > \\
& < current\_data > \\
& < history\_data > \\
& < event > \\
& < property > \\
data\_resource ::= {} & 'Medical\ Device\ Sensors :' \\
& < device\_name >< packet\_length >; \\
& |'Electronic\ Patient\ Record :' \\
& < record\_name >< record\_length > \\
record\_length ::= {} & integer \\
packet\_length ::= {} & integer \\
device\_name ::= {} & ('a'..'z'|'A'..'Z'|'\_')('a'..'z'|'A'..'Z' \\
& |'0'..'9'|'\_') * \\
record\_name ::= {} & ('a'..'z'|'A'..'Z'|'\_')('a'..'z'|'A'..'Z' \\
& |'0'..'9'|'\_') * \\
module\_name ::= {} & ('a'..'z'|'A'..'Z'|'\_')('a'..'z'|'A'..'Z' \\
& |'0'..'9'|'\_')*
\end{aligned}
$$

2) Vital Sign: Current data and history data are captured in construct *current_data* and *history_data* contained in main entity, respectively. Because each packet or record may contain many vital signs corresponding to a set of indexes, the construct *current_data* is refined with a reserved word *current*, and a set of construct *index*. Each *index* specifies the type of value, position, and length of vital sign contained in packet or record. Three basic data types (*Integer, String,* and *Boolean*), and their corresponding array version (*Integer[], String[]*, and *Boolean[]*), are supported. With the position and length of vital signs, and the length of data packet and record, value of vital signs will be located and abstracted exactly.

$$
\begin{aligned}
current\_data ::= {} & 'current' : (< index >) * \\
index ::= {} & < data\_type >< data\_name > \\
& < data\_location > \\
data\_type ::= {} & 'int' | 'bool' | 'string' | \\
& 'int[]' | 'bool[]' | 'string[]' \\
data\_location ::= {} & < data\_position >< data\_length > \\
data\_position ::= {} & 'data\_start\_position :' integer \\
data\_length ::= {} & 'data\_length :' integer
\end{aligned}
$$

The construct *history_data* is refined with a reserved word *history*, and a set of construct *history_index*. Each *history_index* specifies the type of value, initial value, and update rule of this history index. Supported data types for history data are the same with current data. The update rule is some general java statements that abstract the value, according to the previous packets and records. Also, the update rule can be constructed based on the position and length of *current_data*, with an additional integer to denote the number of packets needs to be searched ahead.

$$
\begin{aligned}
history\_data ::= {} & 'history' : (< history\_index >) * \\
history\_index ::= {} & < data\_type >< data\_name > \\
& < abstract\_rule > \\
data\_type ::= {} & 'int' | 'bool' | 'string' | \\
& 'int[]' | 'bool[]' | 'string[]' \\
abstract\_rule ::= {} & < ahead\_num >< data\_position > \\
& < data\_length > \\
& | java - assignment - statement \\
ahead\_num ::= {} & 'previousnumber :' integer \\
data\_position ::= {} & 'data\_start\_position :' integer \\
data\_length ::= {} & 'data\_length :' integer
\end{aligned}
$$

3) Real-Time Event: Event is defined in the fourth construct *event* contained in the main entity. Because vital signs contained in each packet or record may indicate several events, a set of identifiers is used to differentiate them. Traditionally, each event is defined as some boolean expressions on current data. But in case of some temporal properties, event may also use history data. Computations on these data are supported for events related to complex decision logic. We can use just one event with a boolean expression on these data, to release medical staffs from keeping monitoring device screen of Multiple traces.

$$
\begin{aligned}
event ::= {} & 'event :' (< event\_name > \\
& '=' < bool\_exp >) * \\
bool\_exp ::= {} & < current\_data\_name > \\
& | < history\_data\_name > \\
& | < bool\_value > \\
& | < comput\_exp >< compar\_op > \\
& < comput\_exp > \\
& | < bool\_exp > '\&' | '||' < bool\_exp > \\
& | '!' < bool\_exp > \\
& | '(' < bool\_exp > ')'; \\
comput\_exp ::= {} & < current\_data\_name > \\
& | < history\_data\_name >
\end{aligned}
$$

$$
\begin{aligned}
&| < history\_data\_name > \\
&| < int\_value > \\
&| < comput\_exp >< arithe\_op > \\
&< comput\_exp > \\
&|'('< comput\_exp >')'; \\
arithe\_op ::= &'/'|'\%'|'+'|'-'|'*'; \\
compar\_op ::= &'=='|'!='|'<'|'\geq'|'\leq'|'>';
\end{aligned}
$$

4) Temporal Property: Temporal property corresponding to events is defined in the fifth construct *property* of main entity. It consists of two parts, a set of *ptLTL* formulae and handlers. Both parts can be derived from clinical best practice guidelines, such as the logic description part of Arden. Some newly developed medicine knowledge that are not presented in current clinical guidelines can also be encoded into these two parts. The *ptLTL* formulae provide ability to describe most static and temporal conditions, and the handlers will take the result of verification to produce timely response to medical staffs. Besides the standard temporal operators, extra temporal operators such as *"eventually," "always," "always in the past,"* and *"eventually in the past"* denoted as F, F^{-1}, G, and G^{-1}, are also explicitly encoded in the construct. If the property is violated, suggested actions and statements within the handler will be executed, and the runtime monitor would be reset to the initial state automatically. The warnings as well as some status information can be encoded in the handler construct through some print statements of standard Java language.

$$
\begin{aligned}
property ::= &'property:' \\
&(< propoety\_name >'='\\
&< ptLTL\_exp >< handler >)*; \\
ptLTL\_exp ::= &\ event\_name \\
&|N\ ptLTL \\
&|\neg ptLTL\_exp \\
&|X\ ptLTL\_exp\,|\,X^{-1}\ ptLTL\_exp \\
&|F\ ptLTL\_exp\,|\,F^{-1}\ ptLTL\_exp \\
&|G\ ptLTL\_exp\,|\,G^{-1}\ ptLTL\_exp \\
&|ptLTL\_exp \wedge ptLTL\_exp| \\
&ptLTL\_exp\ S\ ptLTL\_exp \\
&|ptLTL\_exp\ U\ ptLTL\_exp \\
handler ::= &\ java - statement \\
model\_name ::= &('a'..'z'|'A'..'Z'|'\_')('a'..'z'|'A'..'Z'| \\
&'0'..'9'|'\_')*;
\end{aligned}
$$

Based on those syntax definitions presented previously, we can build a scenario module within a DRTV model. Real-time vital signs and complex temporal restrictions on these signs of patient could be described in a structured manner. Then, the runtime monitor, consisting of the data parser, event path generator, and property verifier will be formalized and generated automatically from a developed engine, as described in the following subsection.

C. Semantics and Monitor Formalization

With scenarios described in the DRTV model, we need to define the semantics to formalize the data, event, event paths, and property verifier automata for computer interpretable formal verification as follows.

1) Vital Data Formalization: For the current data, which are corresponding to the vital signs of patient, they are formalized as a variable set $\mathbb{D}$ derived from the construct *current_data*. The type of each data d derived from the construct *data_type* is denoted as $T(d)$, where $T(d) \in \{$*Integer, String, Boolean, Integer[], String[], Boolean[]*$\}$.

In the same way, we can formalize the history data. They are formalized as a variable set $\mathbb{D}^h$ derived from the construct *history_data*, and the type of each data d^h is the same with their corresponding current data d. For each variable $d \in \mathbb{D}$, there may be several $d_i^h \in \mathbb{D}^h$ used to capture different time nodes of history. For the history variable, extending its assignment with some general computations on history values is optional for complex restrictions. Assignment of the data set is dependent on the information contained in sampled packets and records, formalized as below.

Formalization 1: θ is a full assignment to $\mathbb{D}$ on the domain of type, where $\theta(d)$ is the value of data d contained in θ, which is derived from the data_location construct. θ^h is a full assignment to $\mathbb{D}^h$, where $\theta(d^h)$ is the value of data d^h contained in θ^h, which is derived from the abstract_rule construct

where θ is a new sampled data packet or a new electronic patient record item, and θ^h is a previously sampled packet or history record.

2) Real-Time Event Formalization: After the data value assignment is abstracted from data packets or records, boolean expressions described in the construct *bool_exp* should be evaluated to get the event set initialized. All events indicated in a data packet or record need to be addressed correctly. Let $\mathbb{E}$ be a set of events derived from the construct *event_name*, and the dataset related to the event set is denoted as $\mathbb{D}_{\mathbb{E}}$, where $\mathbb{D}_{\mathbb{E}} \in \mathbb{D} \cup \mathbb{D}^h$. Then, the event set is formalized as follows.

Formalization 2: $\forall e \in \mathbb{E}$, e is a full assignment to the boolean expressions on $\mathbb{D}_{\mathbb{E}}$. Event e is said to be happened when the assignment is evaluated to be true, which is denoted as $e(\theta(\mathbb{D}_{\mathbb{E}})) == true$.

For event path, it is more complex, because each packet or record may indicate more than just one event corresponding to different indexes. The path should be defined as a sequence of set, where each set a_i is the combination of events evaluated to be true. It is a subset of all events contained in $\mathbb{E}$. Then, the event path is formalized as follows.

Formalization 3: π^* is the group of all finite set sequence π ($\pi = \pi_1\pi_2\pi_3\cdots\pi_n$), and π^ω is the group of all infinite set

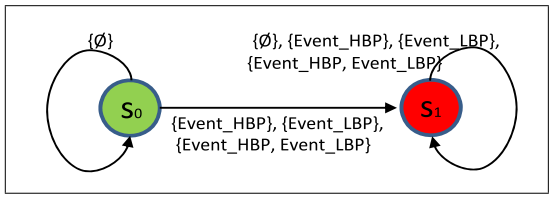


Fig. 4. Formalized monitor automaton.

sequence $\pi^{'}(\pi^{'} = \pi_1^{'}\pi_2^{'}\pi_3^{'}\cdots)$. *Each* π_i *contained in the set sequence is the event combination evaluated to be true in the data packet or record* θ_i, *denoted as* $\pi_i = \{e_j | e_j(\theta_i(\mathbb{D}_{\mathbb{E}})) = true\}$ *and obviously* $\pi_i \in 2^{\mathbb{E}}$. *Furthermore, if* $\forall i \in [1, n], \pi_i = \pi_i^{'}$, *then* $\pi_i^{'}$ *is an extension of* π. *All possible extensions of the finite path* π *are denoted as* $\Sigma(\pi)$.

3) Temporal Property Formalization: The property derived from the construct *property* is the verifier that partitions path into three types, *violation*, *validation*, and *unknown*. Then, the property verifier is formalized as follows.

Formalization 4: A property verifier derived from the ptLTL formula ϕ *is a full assignment to* π^* *on the domain* {*violation, unknown, validation*}, *where* $\forall \pi \in \pi^*$, *the assignment rule is as follows.*

1) *If* $\forall \pi^{'} \in \Sigma(\pi), \pi^{'} \models \phi$, *then* $\phi(\pi) = validation$.
2) *If* $\forall \pi^{'} \in \Sigma(\pi), \pi^{'} \not\models \phi$, *then* $\phi(\pi) = violation$.
3) *Else* $\phi(\pi) = unknown$.

Condition of the assignment rule can be realized by the equivalent monitor automata of the *ptLTL* formula, which can be customized and automatically generated within MOP. The automaton formalized as follows is used to monitor the event sequences defined on the real-time vital signs of patient, and the condition $\pi^{'} \models \phi$ is satisfied when the corresponding path is accepted by the following.

Formalization 4: The customized monitor automaton corresponding to the plLTL formula ϕ *is defined as a tuple* $\langle S, s_0, \alpha, L, O\rangle$.

1) $S = \{s_0, \cdots, s_n\}$ *is the set of states.*
2) s_0 *is the initial state.*
3) $\alpha = \{\alpha_0, \cdots, \alpha_n\}$ *is the set of events contained in the formula* ϕ, *and* $\alpha_i \in 2^{\mathbb{E}}$.
4) $L = \{l_0, \cdots, l_n\}$ *is the transition, and* $l_i \in S \cdot \mathbb{E} \cdot S$.
5) $O = \{o_0, \cdots, o_n\}$ *is the output that maps the state to* {*violation, validation, and unknown*}.

Take the scenario presented in Fig. 3 as an example. If there is a requirement that patient is not allowed to exceed the safe threshold of blood pressure, which can be defined on events $Event\_HBP$ and $Event\_LBP$. This requirement can be formalized as a *ptLTL* formula presented as follows:

$$[\,](notEvent\_HBP \wedge notEvent\_LBP).$$

Then, the customized and generated monitor automaton corresponding to this formula is depicted in Fig. 4. The automaton will start in the initial state s_0. When any of the event sets labeled on the transition happens, such as {*Event_HBP*} or {*Event_LBP*}, or both of them {*Event_HBP, Event_LBP*}, the automaton will transit to violation state s_1. If there is no event, the automaton will stay in the initial state s_0. The automaton only focuses on the event that is related to the property, while others will not be considered for efficient path classification.

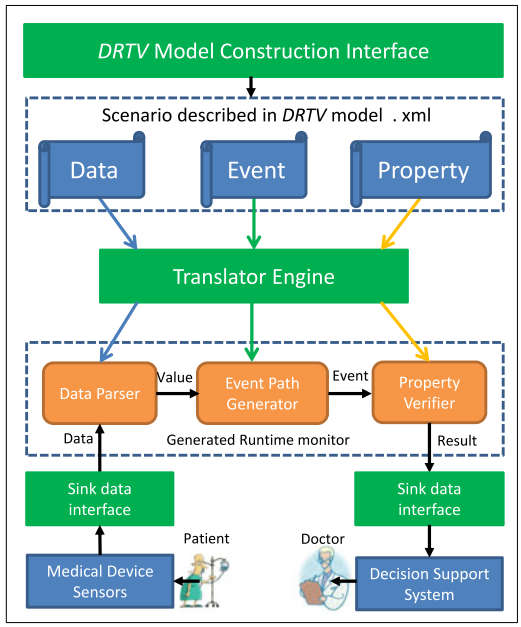


Fig. 5. Tool implementation and interaction. The green modules are implemented components, the yellow modules are generated automatically, the blue files are input by the domain model engineers, and the blue modules are existing DSSs or medical device sensors.

4) Tool Implementation: Based on aforementioned syntax and formalization semantics, we implement an interface for DRTV model construction and an engine to automatically translate the DRTV model into the executable runtime monitor, which consists of data abstractor, event sequence generator, and property verifier. The interface also contains a backend to help validate the syntax correctness and store the model in XML format. Then, the translator contained in the engine will parse the XML file to executable java files. In order to get real-time data from the medical devices or electronic patient recode systems, we also develop a communication interface Sink for data transfer [18]. The overall structure of the tool implementation and interface cooperation is presented in Fig. 5.

IV. Experiment Results

In order to evaluate the efficiency and scalability of the proposed real-time-data-based runtime verification technique, we apply it to the best practice guidelines of real medical care scenarios, then accomplish some real medical-device-based simulation with the closed collaboration of Carle Foundation Hospital. We conduct experiments and generate different runtime verifiers with consistency to a previous developed DSS,[1] which contains integrated workflow, data to decision pipeline, and Medical Device Plug and Play (MDPnP).

[1]The system and related video is presented in http://publish.illinois.edu/mdpnp-architecture/advanced-situation-awareness/

```
Scenario : Stroke_Care
  Medical Device Sensors : intellivue mp70  Data Length : 64;
    Current :
        Int Blood_Pressure , Data Start : 8 , Data Length : 8;
        Int Heart_Rate, Data Start : 8 , Data Length : 8;
    Event :
        Event_UNBP  = (Blood_Pressure > 180  || Blood_Pressure < 90 );
        Event_UNHR  = (Heart_Rate > 120  ||  Heart_Rate < 60 );
    Property:
        SafeState = [](not (Event_UNBP \/ Event_UNHR );
        Handler_SafeState{
            Print("Blood :"+Blood_Pressure+"Heart:"+ Heart_Rate);
            Print("Warnings!!!" + ring());
        };
End Scenario
```

Fig. 6. DRTV model for the blood pressure and heart rate runtime verification, where EVENT_UNBP and EVENT_UNHR denotes the unnormal events leading to property violation.

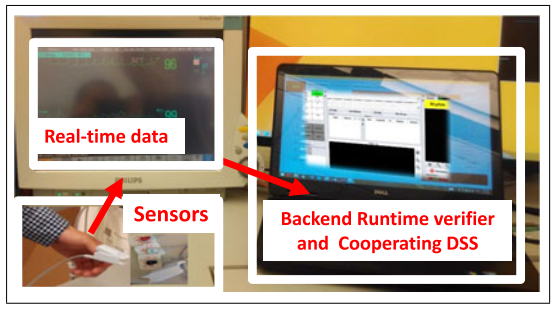


Fig. 7. Real data-based runtime simulation and verification.

The first scenario for test is a best practice guideline recommendation for stroke care [15]. According to the guideline, for the ischemic stroke patient who meets proper criteria [12], administration of IV rt-pa is recommended in a dose of 0.9 mg/kg (maximum of 90 mg), with 10% of the total dose given as an initial bolus and the remainder infused over 60 min. Since a major risk for patient using IV rt-PA is the complication of brain hemorrhage, patient's neurological symptoms such as speech difficulty, facial droop, weakness in hands, and vital signs such as the blood pressure, heart rate, SpO2, and blood glucose level index will be monitored in real time. If any of the vital signs are out of range, stroke team will issue corresponding treatment orders.

For example, when the patient's blood pressure exceeds the safe threshold 180, the stroke team may suggest injecting nitroprusside to control the blood pressure. If the nitroprusside infusion causes the neural deterioration, the physician may change the drug accordingly. If blood pressure and blood glucose level cannot be controlled under acceptable ranges, or signs of brain hemorrhage appear, the stroke team may stop the rt-PA and adjust its schedule to treat complications. Timely response based on the real-time data monitoring and runtime rigorous verification is highly desirable, because every second the huge number of brain cells die, for example, 32 000 brain cells will die within every second a clot blocks blood flow to brain. It is not easy for staff to keep the neurological testing and vital sign monitoring for a long time, but a simple DRTV model segment for blood pressure and heart rate runtime verification can be modeled, as presented in Fig. 6.

Other data parameters such as SpO_2 and temperature, and some corresponding events corresponds to this scenario can also be declared in the model. Those kind of static properties can also be supported by existing DSSs such as Spock and CREDO. But for some temporal properties such as when an event indicates the high blood pressure, the following event must indicate the nitroprusside injection, it can also be defined as

$$[](Event\_HBP\ X\ Event\_Nitroprusside)$$

which is not supported in Spock and CREDO. Then, the generated runtime verifier will be used to verify the real-time data, and produce the timely response automatically, as presented in Fig. 7. The real-time data monitor device Phillips IntelliVue MP70 with the sensors attached on it are used to sensor the real-time data, and the derived runtime verifier of the DRTV model and the data interface are running on the computer. With the developed data interface and MDPnP driver, we continually get the data from Phillips IntelliVue Mp70 and pass them to the generated runtime verifier or our implemented DSS directly. Initially, the real-time data sampled from myself will not violate the property described in Fig. 6. It is not easy to adjust my blood pressure 118 to trigger the violation of property, so inverting the property for testing is adopted in lab simulation. When the property verified is $[]\,Event\_UNP$, timely warnings is produced immediately.

We also do tests on some more complex guidelines, such as the guideline of infants respiratory distress syndrome. If the blood-gas values are too steep for at least 30 s, warnings and further actions should be taken. It is not easy to decide the condition continuously steep of 30 s with semiautomated manual vision inspection. But with the proposed lightweight runtime verification technique, it can be automatically monitored by the following $ptLTL$ formula encoded in DRTV model.

$$[](\underbrace{Event\_Steep\_BG\ X\ \cdots X\ Event\_Steep\_BG})$$

where $Event\_Steep\_BG$ is defined as a boolean expression on two consecutive data packets $(BloodGlas - BloodGlas_1^h \geq Steep\_Threshold)$, one for current data packet and one for the history data packet. When there are 30 number of consecutive steep blood-gas incensement, the property would be violated, and timely warning will be responded immediately.

After those aforementioned tests in the lab, we do some real simulations and verification on virtual patient in hospital, as described in Fig. 8. We use SimMan patient simulator to set the vital signs of virtual patient and the value of real-time data monitor device Phillips IntelliVue MP70, which can be furthered passed to the cooperating DSS and generated runtime verifier. In this way, more guideline properties for potential complications can be verified with different kinds of values set by the SimMan patient simulator, and the results come as expected the same as our previous test.

Furthermore, we choose three typical properties to help us test the efficiency, with results presented in Table I. The first column of Table I is the property name that is defined in the lab test previously, the second column is the number of violations we

Fig. 8. Experiments with the cooperation of SimMan patient simulator in Carle Foundation Hospital.

TABLE I
DETECTED WARNING COMPARISONS FOR DIFFERENT SCENARIOS, AND THE SYMBOL ∅ MEANS NOT SUPPORT. THE LAST TIME IS THE RESPONSE TIME OF MILLISECOND

Property	Number	Manually	DRTV	Spock	Time
UN_HBP	10	10	10	10	1.2
Steep_BG_20	10	10	10	∅	1.4
Steep_BG_30	10	9	10	∅	1.9
UN_HBP	100	94	99	100	1.2
Steep_BG_20	100	81	98	∅	1.5
Steep_BG_30	100	76	98	∅	2.0
UN_HBP	1000	931	992	991	1.3
Steep_BG_20	1000	773	993	∅	1.5
Steep_BG_30	1000	645	992	∅	1.9

insert into the virtual patient through SimMan patient simulator, the third column is the violations manually detected by staring at real-time data monitor device, the fourth column is the violations detected with the accompanied runtime verifier, and the fifth column is the violations detected with the accompanied Spock DSS. From the trend of the third column, we can find that the accuracy of nurse decreases along with the complexity of the property and the work time. For the runtime verifier, it performs steadily as in fourth column. Noting that the DRTV and Spock will produce 10, 100, or 1000 number of warnings, but one or two percent may also be ignored because of noise or other effects that disturb. According to the simulation, it is reasonable to draw the conclusion that the lightweight runtime verifier cooperating with the existing DSS running on the computer helps produce an easier health care practice.

V. DISCUSSION

A. Physicians Need More Flexible and Automatic Support Techniques to Release Them From the Huge Number of Data and Human Tasks During the Clinical Health Care

Nowadays, along with the development of medicine science, more and more medical devices are placed in the ward to provide the information to assist in making decision. However, these devices provide an extra dimension of information for physicians to process. Physician can misread, miss interpret, mixed use the provided information or recall incorrect knowledge to make a decision, during the increasingly common case of continues long-time stressing work.

For example, the work [23] shows that, although medical staffs practice the best practice for cardiac arrest resuscitation, due to its urgent and infrequency on a daily basis, medical staffs may be panic at the situation and miss several warnings. Our experiments also support the conclusion of the aforementioned work, and further show that current DSS does not perform that much good when coming to complex properties, and recently developed computer technology needs to be incorporated. We make use of runtime verification technique, to release physicians from tremendous pressure to relate the information contained in complex medical care systems with temporal properties by semiautomated manual vision inspection of current DSS.

B. Easy to Use Interfaces are Needed to Facilitate Physicians to Use Formal Verification

Through the verification, if we specify the requirements correctly and the data can be intercepted correctly, the false negative and positive rate is almost zero. The specification as well as the violation action definition require the cooperation of doctors, and are highly dependent on medical care practice scenario. Inappropriate property specification and the violation action would reduce the efficiency Computer technologies such as runtime verification and domain specification language are totally new to physicians, we need user-friendly interfaces to convince and facilitate physicians to believe and use those techniques. Currently, it is not possible for physicians to pay extra efforts to learn those techniques due to a huge amount of clinical works, we need to reduce their work by hiding details of implementation techniques and provide the least complex interface.

For example, during the design of DRTV, we plan to use syntax similar to java, which can be more easily connected to the backend MOP. but the physicians from Carle Foundation Hospital thought that it is not easy for them to understand and build the model. Hence, we reduce their efforts by searching many description languages used in current medical DSS, and inherit some syntax from them with assigning MOP-related semantics. Also, the physicians suggest that it would be better for us to provide some templates to translate the property described in the medical best practice guideline to the property described for in DRTV in our future work, which will facilitate their practice of our approach in their health care practices. If the scenario modeling process can be accomplished by automatical generation based on the configuration of medical best practice guideline and devices, it will be more fascistic for them.

VI. CONCLUSION

We propose a lightweight real-time-data-based runtime verification technique for wireless medical cyber-physical system. First, a user-friendly domain specific language DRTV for specifying the real-time data and complex temporal properties of the

medical care practice is designed. Based on the DRTV model, a runtime verification technique is proposed and formalized to strengthen the medical DSS. It combines formal methods in software engineering and practice guidelines in medicine to rigorous verify runtime temporal properties automatically, and can be implemented and plugged in existing wireless medical cyber-physical system to strength the health care.

References

[1] D. Arney, M. Pajic, J. M. Goldman, I. Lee, R. Mangharam, and O. Sokolsky, "Toward patient safety in closed-loop medical device systems," in *Proc. ACM/IEEE 1st Int. Conf. Cyber-Phys. Syst.*, 2010, pp. 139–148.

[2] A. Bauer, M. Leucker, and C. Schallhart, "Runtime verification for LTL and TLTL," *ACM Trans. Software Eng. Methodol.*, vol. 20, no. 4, pp. 619–635, Sep. 2011.

[3] L. Bu, Q. Wang, X. Chen, L. Wang, T. Zhang, J. Zhao, and X. Li, "Toward online hybrid systems model checking of cyber-physical systems' time-bounded short-run behavior," *ACM SIGBED Rev.*, vol. 8, no. 2, pp. 7–10, 2011.

[4] F. Chen and G. Roşu, "Java-mop: A monitoring oriented programming environment for java," in *Tools and Algorithms for the Construction and Analysis of Systems*. Berlin, Germany: Springer-Verlag, 2005, pp. 546–550.

[5] P. A. De Clercq, J. A. Blom, H. H. Korsten, and A. Hasman, "Approaches for creating computer-interpretable guidelines that facilitate decision support," *Artif. Intell. Med.*, vol. 31, no. 1, pp. 1–27, 2004.

[6] J. Fox, V. Patkar, and R. Thomson. "Decision support for health care: The proforma evidence base," *Inf. Primary Care*, vol. 14, no. 1, pp. 49–54, 2006.

[7] G. Hripcsak, P. D. Clayton, T. A. Pryor, P. Haug, O. Wigertz, and J. Van der Lei, "The arden syntax for medical logic modules," in *Proc. Annu Symp. Comput. Appl. Med. Care*, 1990, pp. 200–204.

[8] D. Isern and A. Moreno, "Computer-based execution of clinical guidelines: A review," *Int. J. Med. Informat.*, vol. 77, no. 12, pp. 787–808, 2008.

[9] Y. Jiang, H. Liu, H. Kong, R. Wang, M. Hosseini, J. Sun, and L. Sha, "Use runtime verification to improve the quality of medical care practice," in *Proc. 38th ACM Int. Conf. Software Eng*, 2016, pp. 112–121.

[10] G. Kiczales, E. Hilsdale, J. Hugunin, M. Kersten, J. Palm, and W. G. Griswold, "An overview of aspectJ," in *Proc. Eur. Object-Oriented Program.*, 2001, pp. 327–354.

[11] A. L. King, L. Feng, O. Sokolsky, and I. Lee, "A modal specification approach for on-demand medical systems," in *Foundations of Health Information Engineering and Systems*. Berlin, Germany: Springer-Verlag, 2014, pp. 199–216.

[12] M. G. e. Lansberg, "Antithrombotic and thrombolytic therapy for ischemic stroke: Antithrombotic therapy and prevention of thrombosis: American college of chest physicians evidence-based clinical practice guidelines," *CHEST J.*, vol. 141, pp. e601S–e636S, 2012.

[13] T. Li, F. Tan, Q. Wang, L. Bu, J.-n. Cao, and X. Liu, "From offline toward real-time: A hybrid systems model checking and cps co-design approach for medical device plug-and-play (MDPnP)," in *Proc. IEEE/ACM 3rd Int. Conf. Cyber-Phys. Syst.*, 2012, pp. 13–22.

[14] T. Li, F. Tan, Q. Wang, L. Bu, J.-N. Cao, and X. Liu, "From offline toward real time: A hybrid systems model checking and CPS codesign approach for medical device plug-and-play collaborations," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 642–652, Mar. 2014.

[15] P. Lindsay *et al.*, "Canadian best practice recommendations for stroke care (updated 2008)," *Can. Med. Assoc. J.*, vol. 179, no. 12, pp. S1–S25, 2008.

[16] H. Lu and A. Forin, "The design and implementation of p2v, an architecture for zero-overhead online verification of software programs," Microsoft Research Tech. Rep. MSR-TR-2007-99, 2007.

[17] P. O. Meredith, D. Jin, D. Griffith, F. Chen, and G. Roşu, "An overview of the mop runtime verification framework," *Int. J. Software Tools Technol. Transfer*, vol. 14, no. 3, pp. 249–289, 2012.

[18] H. Mohammad, Y. Jiang, W. Poliang, B. Richard, and S. Lui, "Sink: A middleware for synchronization of heterogeneous software interfaces," in *Proc. 14th Workshop Adaptive Reflective Middleware*, 2015, pp. 1–6.

[19] M. Pajic, I. Lee, R. Mangharam, and O. Sokolsky. "Upp2sf: Translating uppaal models to simulink," Univ. Penn., Tech. Rep. 2011072, 2011.

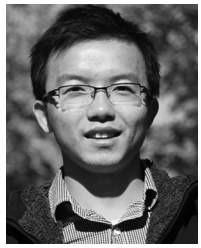
[20] M. Pajic, R. Mangharam, O. Sokolsky, D. Arney, J. Goldman, and I. Lee, "Model-driven safety analysis of closed-loop medical systems," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 3–16, Feb. 2014.

[21] R. Pellizzoni, P. Meredith, M. Caccamo, and G. Rosu, "Hardware runtime monitoring for dependable cots-based real-time embedded systems," in *Proc. Real-Time Syst. Symp.*, 2008, pp. 481–491.

[22] S. Quaglini, P. Ciccarese, G. Micieli, and A. Cavallini, "Non-compliance with guidelines: Motivations and consequences in a case study," *Stud. Health Technol. Inf.*, vol. 101, pp. 75–87, 2003.

[23] N. Strzyzewski, "Common errors made in resuscitation of respiratory and cardiac arrest," *Plastic Surg. Nurs.*, vol. 26, no. 1, pp. 10–14, 2006.

[24] O. Young, Y. Shahar, Y. Liel, E. Lunenfeld, G. Bar, E. Shalom, S. B. Martins, L. T. Vaszar, T. Marom, and M. K. Goldstein, "Runtime application of hybrid-Asbru clinical guidelines," *J. Biomed. Inf.*, vol. 40, no. 5, pp. 507–526, 2007.



Yu Jiang received the B.S. degree in software engineering from the Beijing University of Post and Telecommunication, Beijing, China, in 2010, and the Ph.D. degree in computer science from Tsinghua University, Beijing, in 2015.

He is currently a Post-Doctoral Researcher with the Department of Computer Science, University of Illinois at Urbana-Champaign, Champaign, IL, USA. His current research interests include domain specific modeling, formal computation model, formal verification and their applications in embedded systems, and safety analysis and assurance of cyber-physical system.

Houbing Song received the M.S. degree in civil engineering from the University of Texas, El Paso, TX, USA, in 2006, and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012.

In 2012, he joined the Department of Electrical and Computer Engineering, West Virginia University, Morgantown, WV, USA, where he is currently an Assistant Professor. His current research interests include cyber-physical systems, intelligent transportation systems, wireless communications and networking, and optical communications and networking.

Rui Wang received the B.S. degree in computer science from Xi'an Jiaotong University, Xi'an, China, in 2004, and the Ph.D. degree in computer science from Tsinghua University, Beijing, China, in 2011.

She is currently an Associate Professor with the College of Information Engineering, Capital Normal University, Beijing. Her current research interests include formal verification and their applications in embedded systems.

Ming Gu received the B.S. degree in computer science from the National University of Defense Technology, Changsha, China, in 1984, and the M.S. degree in computer science from the Chinese Academy of Science, Shengyang, China, in 1986.

Since 1993, she has been working as a Professor with Tsinghua University, Beijing, China. Her research interests include formal methods, middleware technology, and distributed applications.

Jiaguang Sun received the B.S. degree in automation science from Tsinghua University, Beijing, China, in 1970.

He is currently a Professor with Tsinghua University, where he is also the Director of the School of Information Science and Technology and the School of Software. He is dedicated in teaching and research and development activities in computer graphics, computer-aided design, formal verification of software, and system architecture.

Lui Sha received the Ph.D. degree in computer science from Carnegie Mellon University, Pittsburgh, PA, USA, in 1985.

He is currently a Donald B. Gillies Chair Professor of Computer Science with the University of Illinois at Urbana Champaign, Champaign, IL, USA. His work on real-time computing is supported by most of the open standards in real-time computing and has been cited as a key element in the success of many national high-technology projects including GPS upgrade, the Mars Pathfinder, and the International Space Station.