A Review of Formal Methods for Intelligent Adaptive Systems with an Application to Intelligent Water Level Monitoring System*

Pranali S. Tekale,
NIT Trichy,India.
tekale.pranali@gmail.com

Ramakalyan Ayyagari,
NIT Trichy,India.
rkalyn@nitt.edu

S D Sudarsan ,
ABB Bangalore,India.
sudarsan.sd@in.abb.com

Raoul Jetley,
ABB Bangalore,India.
raoul.jetley@in.abb.com

ABSTRACT

Intelligent adaptive systems are sensitive to their environment, which enables them to address the complexity of modern software systems. As a result, they are able to adapt to changes in the environment autonomously. Numerous algorithms are available to provide adaptivity to the system. However, formal methods have not been widely used for specification and verification of adaptive systems. Our main aim is application of formal methods to the intelligent adaptive systems to ensure correctness of system design. In this paper, we present a case study of intelligent water level monitoring system. UPPAAL model checking tool is used for formal specification, modelling and verification of the presented case study. Also counter example analysis is used to identify sources of two problems in the system design.

KEYWORDS

Adaptive system, intelligent water level monitoring system, formal methods, formal specification, formal verification, modelling, UPPAAL, sensors, timers.

1. INTRODUCTION

Intelligent adaptive systems adapt to changing environments as well as the users they interact with, so that they can communicate efficiently and naturally with them. They are expected not only to automatically acquire knowledge through a variety of intelligent tools and technologies but also to learn and optimize their behavior over time. They can be used in a large number of applications such as intelligent transportation systems, smart Grid, smart logistics, smart environmental protection, smart home, smart medical, smart safety, industrial automation, smart agriculture etc. [1].

In this paper, we present a case study on water level monitoring system for residential consumers. It uses UPPAAL model checking tool for Formal specification and verification of the proposed system. This system has three different monitoring mechanisms which ensure its adaptive behavior in the diverse changing environments. These environments are not necessarily exhaustive as exemplified in the paper. The remainder of the paper is organized as follows. Section 2 provides the background including a short introduction to formal methods and its key elements. Section 3 presents the case study on intelligent water level monitoring system. Formalization of the case study using UPPAAL is explained in detail in section 4. Section 5 concludes the paper.

The architecture proposed in the paper is the very basic architecture but covers a large class of problems (such as factory automation, oil and gas refineries, mining operations, power generation and distribution, to name just a few).

2. BACKGROUND

2.1 Formal methods

Formal methods are mathematics based techniques for describing system properties. They provide frameworks within which people can specify, develop, and verify systems in a systematic manner. They help identify errors, ambiguities and problems in the early stages of the system development process [2].

Key elements of Formal methods

2.1.1 Formal Specification

It is a complete representation of the system under study using certain formal specification languages. They provide a complete syntax, semantics and pragmatics for its representation. Different specification languages used in developing formal methods are abstract state machines, CSP,LOTOS, RAISE, Rebeca modeling language, SPARK Ada, VDM and Z notation etc.[2,3].

2.1.2 Modelling

In general a model is a mathematical representation of the system under study. They can of different types such as abstract state machine models, automata based models, object oriented models etc. Further automata based models can make use of deterministic finite automata, nondeterministic finite automata, timed automata, Buchi automata, ω-automata etc. These models are used for modelling the formally specified system.

2.1.3 Formal Verification

It is a process of confirming that system under study satisfies its specifications or requirements [2]. It can be achieved by various approaches such as simulation, theorem proving and model checking. They are mainly used to check different system requirements like safety, liveness, deadlock freeness and reachability requirements.

2.1.4 Counterexample analysis

A counterexample has been generated by the model checker, when certain requirements are not satisfied during verification process. It gives relevant information to identify sources of problems

3. THE CASE STUDY ON INTELLIGENT WATER LEVEL MONITORING SYSTEM

Generally residential consumers have an overhead tank whose size depends upon their requirement. They use an electric motor to pump the water from underground to this tank. Since monitoring water level in the tank is a tedious task which requires efficient use of the motor for uninterrupted utility, instead of using conventional ON-OFF control strategy we should incorporate machine control. This eliminates requirement of the human in the loop. Therefore the system becomes automatic. Moreover functionality and adaptive behavior of the system can be separated in the design process.

3.1 Functionality of the system

3.1.1 Principle of working of the water level monitoring unit.

The working principle of the proposed system is illustrated in the fig.1. This construction follows a top down self-adaptive approach. Here the system is centralized, and operates with the guidance of a central control unit. It assesses its own behavior in the current environment and adapts itself whenever its monitoring and analysis systems indicate that it should do so. It consists of four main blocks - the tank, the motor, the sensors and the central adaptive control unit. Here, tank is presumed to be subjected to a number of disturbances by its environment. They are explained in the subsequent sections in the paper.

When water in the tank goes below the specified low level, the motor will be automatically switched ON by the proposed control circuit. Likewise, as soon as water reaches the specified high level in the tank, the control circuit should switch OFF the motor.

High level and low level of the tank are first fixed based on the height and size of the tank for a typical household application. Sensors are presumed to have been fixed at these positions, and they play the role of feedback element in the closed-loop control system. Thus, the construction in fig.1 is a feedback system as well.

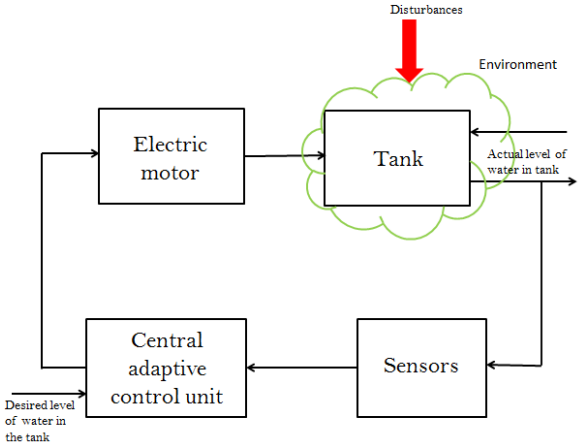

Figure1: Functional block diagram of the system

3.1.2 General layout of the proposed water level monitoring system using Conductive sensors

It is shown in the fig. 2. Its Components are described below

- The liquid level *control unit* is a microcontroller based circuit. It is an electric device with contacts that open and closes in response to liquid levels sensed by the probes. Because it is wired directly to the power source and to the sensing source, it can send signals that activate or deactivate the electric motor.
- The *fitting* is a housing that holds the probes (i.e. conductive sensors).It insulates them from the vessel, and provides a means of connection to the control.
- The *probe* is a sensor that extends downward from the fitting with the tip positioned precisely at the level where the control should be activated.
- *The Motor* is an electrical device which pumps ground water into the tank as per instructions from control circuit [4].

3.1.3 Monitoring mechanisms

Water level can be monitored by three possible ways as shown in fig.3. They are explained briefly below.

I. *Monitoring by conductive sensors unit*

The sensors are made up of 316 stainless steel rods. They are sometimes called as probes. Its working principle is explained in section 3.1.1 and is pictorially represented in fig.2

II. *Monitoring by stainless steel magnetic float level sensors unit*

The sensors are made up of stainless steel magnetic floats. Their working principle is same as for conductive sensors.

III. *Monitoring by ON and OFF delay timer unit*

Generally the timer is a relay having such an output which electrically closes or opens the circuit after a preset time elapses when electrical input is given. This unit makes use of ON and OFF delay operation of the timer [5]. ON and OFF delay timers are assigned values 22.5 and 1.5 hours respectively. These values are based on assumption that it takes approximately 1.5 hours to fill the tank and 22.5 hours to empty the tank.

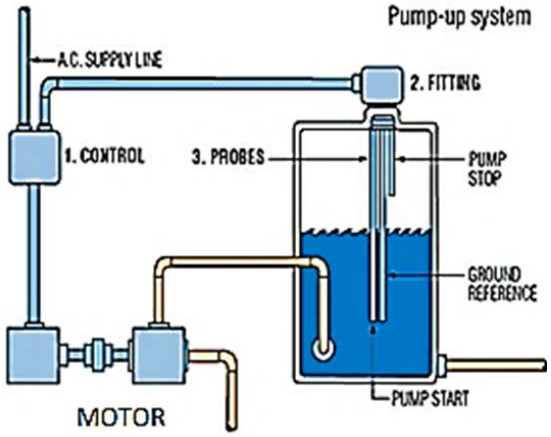

Figure 2: monitoring system using conductive sensors

3.2 Adaptive behavior of the system

First priority for water level monitoring is always given to conductive sensors unit. It is shown by solid line in fig.3.In case of any fault in it, magnetic float sensors and timer circuit monitoring unit will be given the next preference in the same order. It is represented by dotted lines in fig.3. Here faults in any one of the components such as sensors and timers can be regarded as changes in the environment. In this system control unit takes decision autonomously and adapt to these changes. Moreover, the control unit can be connected to a GSM dialer unit to messages about this fault to registered mobile number. Hence consumer can take necessary troubleshooting action for it.

However failure of sensor and timer unit components are not the only changes expected in the current system environment which account for the adaptation. Numerous other changes present in the environment can also be listed, after an observation of the system and the consumer behavior over a certain period of time. For example, we neither mentioned about rating of the electric motor nor faults occurring in it. Its rating and size of the tank depends upon the consumer demand. It depends in turn upon number of people residing in the particular house. Further there is a possibility of leakage in the pipes used to pump water from ground to overhead tank. We can also account for the alternative power supply unit to ensure the continuity of electric supply to the system.

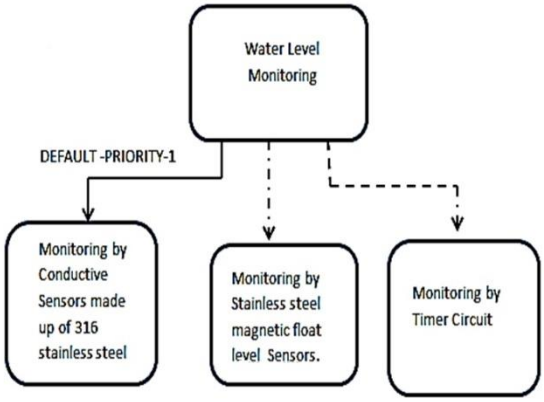

Figure 3: Adaptive behavior of the system

4. FORMALIZATION OF THE CASE STUDY IN UPPAAL

UPPAAL model checking tool is used for formalization of the system [6]. It consists of number of processes for the particular system. Every process is modelled as a grid of timed automata [7]. Further it uses TCTL for defining requirements, known as query language. This language contains state and path formulae. Individual states, with regular expressions such as y >= 0 or y <=0 or y == 0, can be described by state formulae. Path formulae quantify over the path of the model. They can be classified over safety, liveness and reachability properties.

- Safety Properties are used to verify that something bad will never happen.
- Reachability properties are used to check whether a given state formula can be satisfied by some reachable state.
- Liveness properties are used to verify that something eventually will hold

This process of formalization of the system is divided in three steps as discussed in section 2. These steps are explained as follws.

4.1 Formal specification

Some of the safety and reachbility requirements to be formally specified for the case study are listed below.

- The electric motor should be switced ON by any one of the three monitoring units, illustrated in section 3.2.This can be specified by the equation[1] given below
  $(c \wedge \neg f \wedge \neg t) \vee (\neg c \wedge f \wedge \neg t) \vee (\neg c \wedge \neg f \wedge t)$
- There is no deadlock formation in the system.
- All the monitoring mechanisms are expected to be as follows :-
  - If the low level of water in the tank is sensed, then motor should switch ON.
  - If the high level of water in the tank is sensed, then motor should switch OFF.
  - At no point, both low and high level sensors should become zero or one simultaneously.

4.2 Modelling

All the elements of water level monitoring system shown in fig. 1, 2 and 3 are modelled in UPPAAL. These models are explained in following subsections.

4.2.1 Control unit

It consists of five states. *StartOfCycle*[2] state initiates the process of water level monitoring. Three monitoring units using conductive sensors, float sensors and timer circuit are indicated by states *One*, *Two*, Three respectively. Here, state *One* has been marked as an urgent state to indicate its first priority in the monitoring process. Also variables c, f and t are used to indicate the current mode of operation of three monitoring units conductive sensors(c), float sensors(f) and timer circuit (t) respectively. These monitoring units can operate in either normal or faulty mode. Whenever they operate in normal mode, value zero should be assigned to all the three variables and whenever they operate in the faulty mode, value one should be assigned to them. Further synchronization channels Activate1, Activate2 and Activate3 are used to communicate to the process models of the corresponding monitoring units. This unit is shown in fig.4.

4.2.2 Monitoring unit using conductive sensors

It is a state machine with three states. It is shown in fig.5. Initial state *On_1* initiates the process of Monitoring by Conductive sensors. Remaining two states, *LowLevelElectrode* and *HighLevelElectrode* are used to indicate that the specified low level and high level of the water in the tank is sensed by them respectively.

Start and *Stop* channels are used to communicate to the electrical motor, by giving the command to switch it ON and OFF respectively. It responds to the message *Activate1* from the control unit and then starts its monitoring action.

4.2.3 Monitoring unit using float sensors

This state machines construction and principle of operation is same as conductive sensors monitoring unit. However *LowLevelFloa*t and *HighLevelFloat* are used instead of *LowLevelElectrode* and *HighLevelElectrode respectively.* It should receive *Activate2* message from the control unit to begin its monitoring action. Its pictorial representation is given in the fig.6.

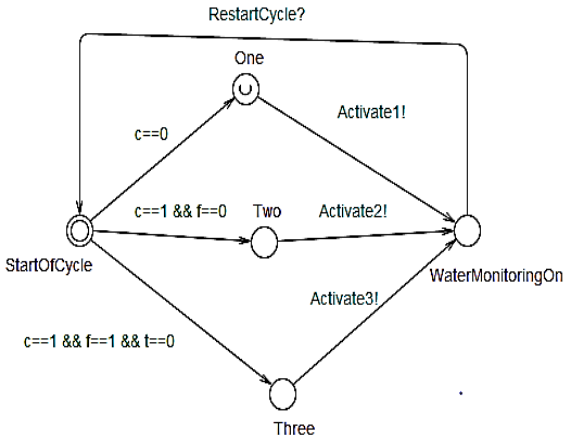

Figure 4: control unit

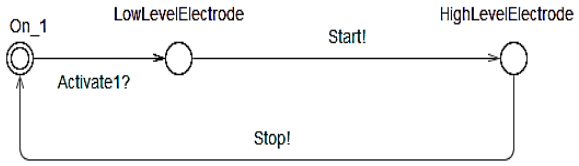

Figure 5: Monitoring by conductive sensors

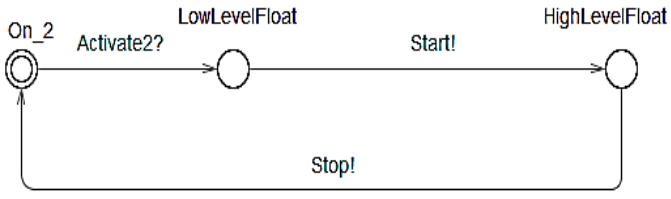

Figure 6: Monitoring by magnetic float level sensors

[1]Detailed descriptions about variables c, f and t are given in the section 4.2.1

[2]All the states and channels shown in figures particularly in the modelling section are shown by italic font in this section.

4.2.4 *Monitoring unit using timer circuit*

Its construction contains 5 states. It is represented in fig.7.

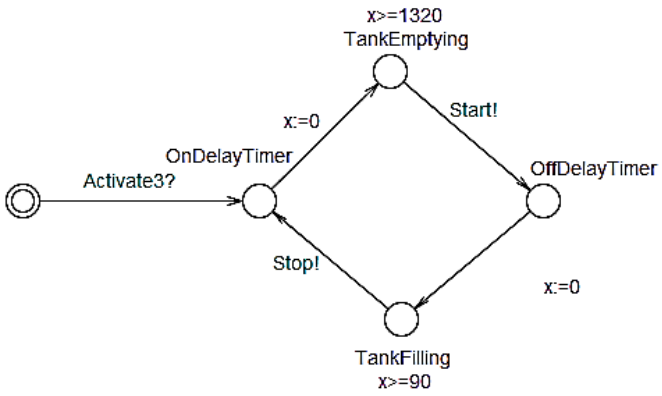

Figure 7: Monitoring by timer circuit

Initial state *On_3* initiates the process of monitoring as soon as it receives message *Activate3* from microcontroller based control unit. States *OnDelayTimer* and *OffDelayTimer* are used to indicate ON and OFF delay operations of the timer respectively. Two intermediate states *TankEmptying* and *TankFilling* are defined for communication with the motor model. For this purpose, it uses *Start* and *Stop* synchronization channels.

4.2.5 *The electric motor*

It consists of only two states *ON* and *OFF*. *OFF* being an initial state will start the motor when it receives message *Start* from one of the three monitoring units .Then it remains in this ON state as long as 90 minutes. It will go back to the *OFF* state after receiving message *Stop* from monitoring unit. Further,to restart the operation of monitoring once again ,state *OFF* is provided with the self loop. For this purpose ,it will send the message *RestartCycle* to the control unit. Diagramatic representation of this unit is shown in fig.8.

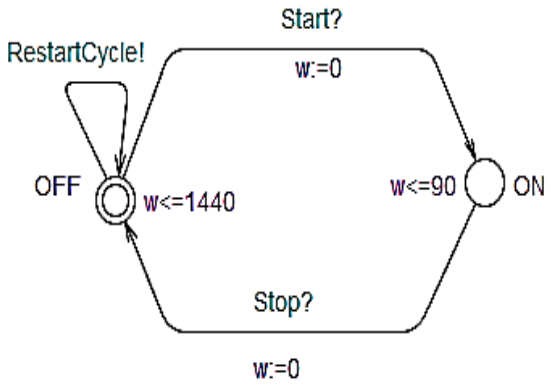

Figure 8: Electric motor

Functional and adaptive behavior of the system modelled in UPPAAL

The control unit is the heart of the proposed system. When the working cycle starts, it immediately makes transition to the state *One* from the initial state, because state *one* is marked as an urgent state and by default variable c is set to zero. In the *One* state, message *Activate1* will be sent to the conductive sensors monitoring unit to initiate the process of water level monitoring. For this purpose, this unit will communicate with the motor unit by sending messages *Start* and *Stop* to it.

If one of the sensors in the conductive sensors unit fails, then variable c will become one. Now float sensors monitoring unit will come in action. If this unit also fails, then timer circuit will perform water monitoring function because variable t still has value zero. In this way, the system modelled in the UPPAAL exhibits the property of adaptation.

4.3 Formal verification

All the safety and reachability requirements formally specified in the section 4.1 are verified in the UPPAAL using A and E state formulae. They are listed as below

- A[ ] not (ElectricMotor.*ON* and (c==1 && f==1 && t==1))
- A[] ElectricMotor.*ON* imply ((c==0 && f==1 && t==1) || (c==1 && f==0 && t==1) || (c==1 && f==1 && t==0))
- A [ ] not deadlock.
- E<> ElectricMotor.*ON* imply Control.*WaterMonitoringOn*
- E<> ConductiveSensors.*HighLevelElectrode*
- E<> ConductiveSensors.*LowLevelElectrode*
- E<> FloatSensors.*HighLevelFloat*
- E<> FloatSensors.*LowLevelFloat*
- E<>TimerCircuit.*OnDelayTimer*
- E<>TimerCircuit.*OffDelayTimer*
- E<> ElectricMotor.*OFF*
- E<> ElectricMotor.*ON*

These properties prove that the system under study satisfy the specified requirements. In other words, they indicate that water level monitoring system work properly and adapt to the specified changes in the environment successfully.

4.4 Counterexample analysis

In UPPAAL, a counterexample can be generated using diagnostic trace option. This counterexample can be used to analyze the sources of problems. Typical problems could be requirement specification or the model of the system itself. In the current case study by using the counterexample, we were able to find the

source of two problems. It turned out that two requirements of the system were not correctly specified. First one is about deadlock formation in the system. As long as one of the three monitoring units are working in the normal operating condition, there was no deadlock formation in the system. But this requirement was not satisfied when all three monitoring mechanisms fail. So the requirement specification:

"A [] not deadlock"

should be modified to

"A [] not deadlock implies ((c==0) ||(c==1 & f==0) ||(c==1 && f==1 && t == 0))"

or

"A [] deadlock imply (c==1 && f==1 && t==1)"

A second problem was found regarding the requirement specification of the motor during switched ON condition. As per the specification in the section 4.1, motor in the switched ON condition indicates that one of the monitoring mechanism, which is working in the healthy operating condition, is activated. But counterexample analysis result showed that motor can't be turned ON by any one of the healthy monitoring unit randomly. Instead, a hierarchy among the units must be maintained according to the adaptive behavior of the designed system. Thus, the requirement specification should be changed to

"A [] ElectricMotor.*ON* imply ((c==0) || (c==1 && f==0) || (c==1 && f==1 && t==0))"

from

"A[] ElectricMotor.*ON* imply ((c==0 && f==1 && t==1) || (c==1 && f==0 && t==1) || (c==1 && f==1 && t==0)) "

5. CONCLUSION

In this paper, we presented the case study of intelligent water level monitoring system. Different safety and reachability requirements of the system are specified, modelled and verified in the UPPAAL model checking tool. Also bugs in the requirements specifications were reported after counterexample analysis. Here failure in the sensors and timers are regarded as changes in the environment. Formal verification process validates the adaptive behavior of the system in defined changing environments. However, there is wide scope for defining various unaccounted changes in the environment and add additional functionality to the present system so that it will adapt to those changes.

REFERENCES

[1] Frank D.macias-escriva, Rodolf Haber, Raul Del Toro, Vicente Hernandez,Self –Adaptive Systems: a survey of current approaches, Research challenges & applications, *Science direct-Expert systems with applications*,2013.

[2] J.M.Wing, A Specifiers Introduction to formal methods, *IEEE computer*,Sep1990.

[3] Edmund M. Clarke, Jeannette M. Wing, Et al, Formal Methods: State of the Art and Future Directions, *ACM Computing Surveys*, Vol. 28, No. 4, December 1996

[4] Gems sensors & controls corporation official website *http://www.gemssensors.com/Level/Warrick/Conductivity-Based-Liquid-Level-Control*

[5] Panasonic corporation official website *http://www3.panasonic.biz/ac/ae/fasys/component/timer/explain_term/*

[6] Bengtsson, J., larsen, K.G., Larsson,F.,Pettersson, P., Yi W., UPPAAL - a Tool Suite for Automatic Verification of Real-Time Systems, *in Proceedings of the 4th DIMACS Workshop on Verification and Control of Hybrid Systems, New Brunswick, New Jersey*, 22-24 October,1995

[7] Alur R., Dill, D.L, Automata for modeling real-time systems, *Colloquium on Algorithms, Languages, and Programming*,1990.