MATEC Web of Conferences **44**, 02092 (2016)
DOI: 10.1051/matecconf/20164402092

A Method for Cyber-Physical System Behavior Modeling and Safety Verification Based on Extended Hybrid System Description Language

Ming Fu Tuo[1,2], Xing She Zhou [1] ,Zheng Xin Guo [3] and Li Jun Shan [1]

[1] *Northwestern Polytechnical University, Xi'An, China*
[2] *Air Force Engineering University, Xi'An, China*
[3] *Hunan University, Changsha, China*

Abstract. The safety of Cyber-physical system(CPS) is up to its behavior, and it is a key property for CPS to be applied in critical application fields. A method for CPS behavior modeling and safety verification is put forward in this paper. The behavior model of CPS is described by extended hybrid system description language(E-HYSDEL).The formal definition of hybrid program(HP) is given, and the behavior model is transformed to HP based on the definition. The safety of CPS is verified by inputting the HP to KeYmarea. The advantage of the approach is that it models CPS intuitively and verify it's safety strictly avoiding the state space explosion

1 Introduction

Cyber Physical System(CPS) are new type of hybrid systems which characterized by deeper integrations of computation with physical processes[1].Application fields of CPS are very wide, such as Intelligent transportation, telemedicine, the smart-grid, aeronautics and astronautics, and so on[2].

Safety is a key property for CPS to be applied in critical application fields. Whether the properties of CPS can satisfies the requirements can be analyzed in the system design stage by model verification technology. This helps to find the defects of deign as early as possible, so it can reduce the risk of system development effectively.

2 Studies of CPS analysis and verification

With the widely used of CPS,the study for CPS analysis and verification becomes more and more deeply.To extend the classical verification methods is one of the ways,such as extention of FSM,optimization of fault tree,etc[3][4].There are also researchers use colored petri nets(CPN) to model and verify CPS.

Formal verification methods,such as model checking and theorem proving,are used to verify safety and other properties of CPS recently[5].Model checking technology determines the authenticity of a proposition by traversing the state space.it's main advantage is a high degree of automation. Furthermore,it can generate counterexample. However, It is difficult to overcome the sate space explosion problem. Cyber-physical systems usually are hybrid systems. They include both discrete states transitions and dynamic continuous variation processes, that is to say the sates of most CPS are infinite.

From the practical point of view, theorem proving method is more suitable for safety verification of CPS[6]. Differential dynamic logic(dL), put forward by Platzer, is one of theorem proving methods. It has been successfully used in fields such as the air traffic control system, European train control system because of its rigorous syntax and clear semantics. The operational model of dL is hybrid program(HP). dL is well supported by KeYmarea, a famous theorem prover.

3 The framework of the method for CPS behaviour modelling and safety verification

In this paper,We extend HYSDEL, a traditional hybrid system description language, and name it E-HYSDEL. Furthermore, we use it to model the behavior of CPS. Based on this, the safety of CPS is verified. The framework of this new method for CPS behavior modeling and safety verification can be depicted as figure 1.

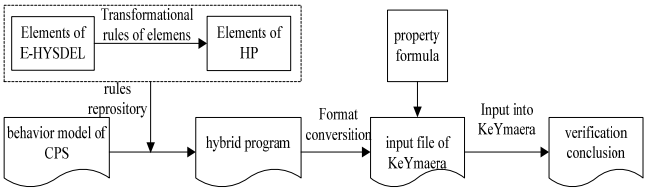

Figure 1. the framework of the CPS behavior modeling and safety verification

According to this framework, the process for CPS behavior modeling and safety verification can be divided into four steps. In the first, the transformation rules between meta-model of E-HYSDEL and meta-model of HP are established. Then, the behavior model of a specific CPS is described by E-HYSDEL code. Next, the behavior model is transformed to the corresponding HP based on the transformation rules. Finally, the formula that describes the constraints of variables affecting safety of system and the HP are inputted into KeYmarea to verify whether the safety related constraints are met.

4 The formal definition of HP

The formal definition of HP is given as follows.

HPM=(PD，VD，PC，SHPS)

PD represents parameter declaration.

VD represents dynamic variables declaration.

PC represents precondition, in other word, the constraints of variables before system runs.

[a] Corresponding author:mftuo@163.com

Article available at http://www.matec-conferences.org or http://dx.doi.org/10.1051/matecconf/20164402092

SHPS represent the set of sub hybrid program. Each SHP is defined as follows.

SHP=(MS，DTS，CTS)

MS represents set of discrete states.

DTS represents set of transitions of discrete states, that is transitions between modes.

CTS represents set of dynamic processes, it describes the continuous change in a single mode.

Some transformational rules are set up based on this formal definition.

5 Application case

Room temperature control system is one of typical CPS(Fig 2).There two persons, a heater, a air conditioning, a window in room. These equipments can affect the room temperature.T1 represents the temperature of place where person 1 stay.T2 represents the temperature of place where person 2 stay. Tamb represents the temperature outside the window. Uhot represents heater power flow when it is on. Ucold represents air conditioning power flow when it is on.

The person 1 turns the heater(air conditioning) on whenever he is cold(heat).If person 2 is cold he turns the heater on unless person 1 is heat. If person 2 is heat he turns the air conditioning on unless person 1 is cold. Otherwise, heater and air conditioning are off.

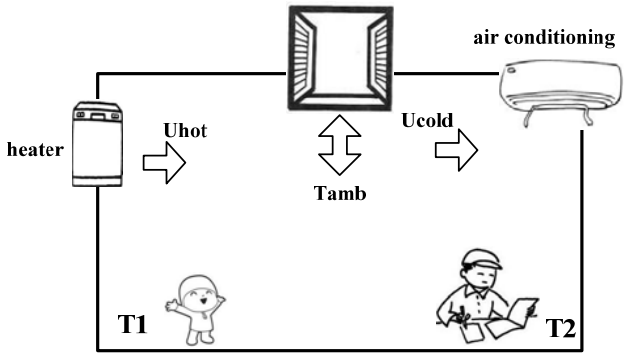

Figure 2. the room temperature system

The changes of T1 and T2 can be expressed by the following equations.

T1′ = -alpha1*(T1-Tamb)+k1*(uhot-ucold)

T2′ = -alpha2*(T2-Tamb)+k2*(uhot-ucold)

In these equations, Ts=0.5，alpha1 = 1，alpha2 = 0.5，k1 = 0.8，k2 = 0.4，Thot1 = 30，Tcold1 = 15，Thot2 = 35，Tcold2 = 10，Uc = 2，Uh = 2.

We will verify the conclusion that state 10≤T1,T2≤ 15 is not reachable on condition that 10≤Tamb≤30 and the initial state is 35≤T1,T2≤40.

The behavior model of temperature control system is described by the following E-HYSDEL codes.

```
SYSTEM heatcool {
INTERFACE {
    STATE {
                REAL T1 [-10,50];
                REAL T2 [-10,50];
            }
    INPUT { REAL Tamb [-10,50]; }
    OUTPUT {
            REAL y1;
            REAL y2;
 }
   PARAMETER
   {
      REAL Ts=0.5, alpha1=1, alpha2=0.5, k1=0.8,
k2=0.4;
    REAL Thot1=30, Tcold1=15, Thot2=35, Tcold2=10,
Uc=2, Uh=2;
    }
}
IMPLEMENTATION {
     AUX {
          REAL uhot, ucold,t;
          BOOL hot1, hot2, cold1, cold2;
      }
     AD  { hot1 = T1>=Thot1;
           hot2 = T2>=Thot2;
           cold1 = T1<=Tcold1;
           cold2 = T2<=Tcold2;
       }
DA  { uhot = {IF cold1 | (cold2 & ~hot1) THEN Uh
ELSE 0
};
       ucold = {IF hot1 | (hot2 & ~cold1) THEN Uc ELSE
0}; }
     CONTINUOUS {
           T1 = T1+Ts*(-alpha1*(T1-Tamb) +k1*(uhot-
ucold));
           T2 = T2+Ts*(-alpha2*(T2-Tamb) +k2*(uhot-
ucold));   }
     OUTPUT {y1=T1;
                 y2=T2;
      }
     }
}
```

The behavior model is transformed to the following HP based on the former transformational rules.

```
heatcool≡（S1∪S2）*
S1≡(
Tamb=*;?(Tamb≥10∧Tamb≤30);
if((T1≤Tcold1)∨(T2≤Tcold2∧¬T1≥Thot1))
uhot:=Uh;
else
uhot:=0;
if((T1≥Thot1)∨(T2≥Thot2∧¬T1≤Tcold1))
ucold:=Uc;
else
ucold:=0;
T1′ = -alpha1*(T1-Tamb)+k1*(uhot-ucold),t′ =1 ;
)
S2≡(
Tamb=*;?(Tamb≥10∧Tamb≤30);
if((T1≤Tcold1)∨(T2≤Tcold2∧¬T1≥Thot1))
uhot:=Uh;
else
uhot:=0;
if((T1≥Thot1)∨(T2≥Thot2∧¬T1≤Tcold1))
ucold:=Uc;
else
```

ucold:=0;
T2′ = -alpha2*(T2-Tamb)+k2*(uhot-ucold),t′ =1 ;
)

Finally, the safety of the system is specified by the formulation ω→ [heatcool*] Φ, where ω is initial condition, and Φ is the conclusion to be verified.

verification used less steps and avoid the state space explosion.

6 Conclusion

The main idea of the given method for behavior modeling and safety verification of CPS is that modeling the behavior of CPS by hybrid automata, which is described by E-HYSDEL language, then transform this model to a corresponding dL model, described by HP, and verify the safety of the dL model by means of KeYmaera.

The advantage of this method is that it models CPS intuitively and verifies it's safety strictly. The method can also be used to verify other property of CPS, such as real-time, reliability.

References

1. Lee, E. *CPS foundations*. Proceedings of the 47th ACM/IEEE Design Automation Conference., 2010. 737−742

ω≡(Tamb≥10∧Tamb≤30)∧(T1≥35∧T1≤40)∧T2≥35 ∧T2≤40)
Φ≡¬((T1≥10∧T1≤15)∨(T2≥10∧T2≤15))

The conclusion is verified in KeYmaera after many steps. The results shows that this method for safety

2. He, J. F. *Cyber-physical systems*. Communications of the China Computer Federation, 2010, 6(1): 25−29
3. Leonardi, F., Pinto, A., and Carloni, L. P. *Synthesis of distributed execution platforms for cyber-physical systems with applications to high-performance buildings*. In: Proceedings of the IEEE/ACM International Conference on Cyber-Physical Systems. Chicago, USA: IEEE, 2011. 215−224.
4. Jha, S., Gulwani, S., Sanjit, A., and Seshia, A. *Synthesizing Switching Logic for Safety and Dwell-Time Requirements*. EECS Department, University of California, Berkeley, Technical Report No. UCB/EECS-2010-28, 2010.
5. Zhu, M., Li, B. X., and Chen, Q. Q., *transforming hybridUML to hybrid program for CPS property verification*. Electronic journals, 2012，40（6）：1126-1132.
6. Platzer，*A Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Heidelberg: Springer, 2010.Luigi T.De Luca, *Propulsion physics* (EDP Sciences, Les Ulis, 2009)