Considering Safety and Feature Interactions for Integrated Services of Home Network System

Ben Yan

Graduate School of Information Science, Nara Institute of Science and Technology
hon-e@is.naist.jp

Abstract. Assuring safety in the home network system (HNS) is a crucial issue to guarantee high quality of life. In this position paper, we first review our previous work, formulating three kinds of safety for the HNS integrated services: *local safety*, *global safety*, and *environment safety*. We then present a method that validates safety for integrated service. Finally, we discuss a perspective in how the safety can be assured when considering the feature interaction problem.

1 Formalizing Safety in Home Network System

The *home network system* (HNS, for short) is comprised of networked home appliances and sensors, which is one of the most promising applications of the emerging ubiquitous computing technologies. The HNS enables flexible integration (or orchestration) of different home appliances and sensors through the network, which achieves value-added *integrated services* [5].

In developing and providing the HNS integrated services, the service provider must guarantee that the service is *safe* for inhabitants, house properties and their surrounding environment. That is, a service is free from any condition that can cause [injury or death to home users and neighbors], or [damage to or loss of home equipments and the surrounding environment].

Since the service is typically implemented as a software application, appliances are often operated automatically by the application, but not by the human user. Also, one integrated service operates multiple appliances, which yields global dependencies among different appliances. Moreover, since multiple integrated services can be executed, unexpected functional conflicts may occur among the services. Thus, a single fault in the service application can cause serious accidents to the user.

In general, the safety is characterized by some *properties* to be satisfied by a user (or a system). In our previous work [6], we have formulated three kinds of safety properties in the context of HNS integrated services.

Local Safety Property A safety property lp is called a *local safety property* iff lp is defined within a single appliance d in the HNS. Typically, lp is derived as a safety instruction for using d. Let $LocalProp(d) = \{lp_1, lp_2, ..., lp_m\}$ be a set of all local safety properties with respect to the appliance d. For a given integrated service s, let $App(s) = \{d_1, d_2, ..., d_n\}$ be a set of networked appliances used by s. Then, we define $LocalProp(s) = \cup_{d_i \in App(s)} LocalProp(d_i)$ which is a set of local safety properties with respect the service s. The following property is an example of the local safety property of an electric kettle:

[L1] *Do not open the lid when the electric kettle is in the boiling mode.*

Global Safety Property A safety property gp is called a *global safety property* iff gp is defined over multiple appliances $d_1, d_2, ..., d_n$. Typically, gp is a safety instruction of an integrated service s that uses $d_1, d_2, ..., d_n$. We denote $GlobalProp(s) = \{gp_1, gp_2, ..., gp_k\}$ to represent a set of all global safety properties for the service s. The following is an example of the global safety property for any integrated service that uses a gas valve and kitchen equipments.

[G1] *While the gas valve is opened, the ventilator must be turned on.*

Environment Safety Property A safety property ep is called an *environment safety property* iff ep is defined as the environmental or residential constraints, which exist independently of any appliances or services. $EnvProp = \{ep_1, ep_2, ..., ep_l\}$ denote a set of all environment properties given. The following environment property might be derived from the safety guideline of the house:

[E1] *The total current used simultaneously must not exceed 30A.*

Safety of HNS Integrated Services Let P be a set of safety properties. For a service s, we write $s \vdash P$ iff s satisfies all properties contained in P. Then, we define the safety of s as follows.

- s is *locally safe* iff $s \vdash LocalProp(s)$.
- s is *globally safe* iff $s \vdash GlobalProp(s)$.
- s is *environmentally safe* iff $s \vdash EnvProp$.
- s is *safe* iff s is locally, globally and environmentally safe.

Thus, the *safety validation problem* is defined as follows:
Input: An integrated service s, $LocalProp(s)$, $GlobalProp(s)$, $EnvProp$.
Output: s is safe or not.

2 Safety Validation by Design by Contract

Since any safety flaws in an integrated service s can lead to serious accidents, we consider it crucial to remove the flaws *before* s is actually deployed in the HNS. In [6], we have proposed a framework of safety validation using object-oriented modeling and *design by contract (DbC)* [4], which is applied to *testing phase* of s. The framework first introduces an object-oriented modeling technique of HNS to clarify the relationships among the HNS components (i.e., appliances, services and the home) [5]. Fig. 1 shows the overview of the proposed model. The model mainly consists of three kinds of objects (classes): `Appliance`, `Service`, and `Home`. These classes forms the following relationships to match well the intuition of the HNS and integrated services: [R1: a `Home` has multiple `Appliances`], [R2: a `Home` has multiple `Services`], and [R3: a `Service` uses multiple `Appliances`].

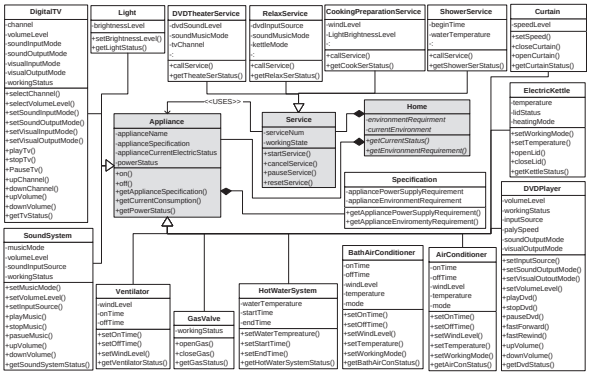

Fig. 1. Object-oriented model of HNS

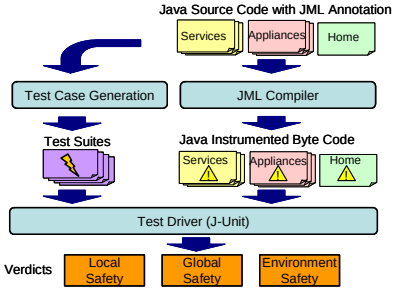

Fig. 2. Safety validation with JML

Assuming that the HNS is implemented according to the model, we then embed the given safety properties into the source code of appropriate objects. For this, we encode each safety property as a *contract* of DbC (i.e., a pre-condition, a post-condition, or a class invariant). More specifically, $LocalProp(s)$, $GlobalProp(s)$ and $EnvProp$ are encoded as certain DbC contracts, and are respectively embedded into `Appliance`, `Service` and `Home` objects. The source code with the DbC contracts are compiled into *instrumented target code* which involves check routines of the contracts. Then, we conduct testing of the instrumented code. While running the testing, if any DbC contract is broken, an exception is thrown and thus the security flaw can be detected. Fig. 2 shows an overview of the safety validation, where the source codes are written in the Java language and the JML (Java Modeling Language) [1, 3] is used for writing the DbC contracts.

3 Feature Interactions and Safety in HNS

The safety validation framework presented above is basically for each individual integrated service, and is executed before the service is deployed in the HNS. However, even if every service is proven to be safe, combined use of multiple services may violate some safety properties, due to *feature interactions* (FIs) among the services. The safety violation by the FIs can be formulated as follows:

For a given pair of integrated services s_1 and s_2,

FI-(L)(Local Safety Violation):

$[s_1 \vdash LocalProp(s_1)] \wedge [s_2 \vdash LocalProp(s_2)] \Rightarrow [s_1{+}s_2 \not\vdash LocalProp(s_1) \cup LocalProp(s_2)]$.

FI-(G)(Global Safety Violation):

$[s_1 \vdash GlobalProp(s_1)] \wedge [s_2 \vdash GlobalProp(s_2)] \Rightarrow [s_1{+}s_2 \not\vdash GlobalProp(s_1) \cup GlobalProp(s_2)]$.

FI-(E)(Environment Safety Violation):

$[s_1 \vdash EnvProp] \wedge [s_2 \vdash EnvProp] \Rightarrow [s_1 + s_2 \not\vdash EnvProp]$.

where the operator $+$ denotes a composition operator of two services [1]. The above

[1] The detailed semantics of the composition are not given here.

definitions the safety violation appear to be quite similar to the definition of the conventional feature interactions in telephony. However, there are some domain-specific issues. Taking them into account, we are currently developing a method for safety validation with FIs.

- The three types of the safety violation could be dealt with different methods.
- The safety properties in HNS must be assured at all costs. There is no *desirable interactions* with respect to the safety violation.
- The formalization of FIs in HNS, presented by Nakamura et al. [5], would contain some cases of the safety violations. However, not all interactions cause a safety violation.
- Our safety validation framework [6] can be used only if both s_1 and s_2 are provided by the same service provider. Otherwise, an alternative online approach is necessary.
- The online approach would be implemented on the central home server, which manages all appliances and environment properties.
- The sophisticated execution control of multiple services (e.g., resource locking [2]) would be promising to prevent FIs that leads to the safety violation. The execution control restricts the semantics of the service composition (i.e., the operator +).

Acknowledgment: This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Young Scientists (B) (No. 18700062) and Scientific Research (B) (No. 17300007), and by JSPS and MAE under the Japan-France Integrated Action Program (SAKURA).

The author thanks to Prof. Masahide Nakamura at Kobe University, Prof. Lydie du Bousquet at Joseph Fourier University, and Prof. Ken-ichi Matsumoto at Nara Institute of Science and Technology, for the supervision of my research.

References

1. L. du Bousquet, Y. Ledru, O. Maury, and P. Bontron, "A case study in JML-based software validation," *Proc. of 19th Int. IEEE Conf. on Automated Software Engineering (ASE'04)*, Linz, pages 294-297, IEEE Computer Society Press, Sep. 2004.
2. M. Kolberg, E. H. Magill, and M. Wilson, "Compatibility issues between services supporting networked appliances", *IEEE Communications Magazine*, vol. 41, no. 11, pp.136-147, Nov. 2003.
3. G. T. Leavens and Y. Cheon, "Design by Contract with JML," Java Modeling Language Project,Internet: http://www.jmlspecs.org, 2003.
4. B. Meyer, "Applying Design by Contract," *IEEE Computer*, vol.25, no.10, pp.40-51, Oct.1992.
5. M. Nakamura, H. Igaki,and K. Matsumoto, "Feature Interactions in Integrated Services of Networked Home Appliances -An Object-Oriented Approach-," *Proc. of Int'l. Conf. on Feature Interactions in Telecommunication Networks and Distributed Systems (ICFI'05)*, pp.236-251, Jul. 2005.
6. B. Yan, M. Nakamura, L. du Bousquet,and K. Matsumoto, "Characterizing Safety of Integrated Services in Home Network System," *Proc. of 5th Int'l. Conf. on Smart homes and health Telematics (ICOST2007)*, pp.130-140, Jun. 2007.