Stepwise Context Boundary Exploration Using Guide Words

Naoyasu Ubayashi[1] and Yasutaka Kamei[1]

Kyushu University, Japan
ubayashi@acm.org, kamei@ait.kyushu-u.ac.jp

Abstract. Most requirements elicitation methods do not explicitly provide a systematic way for deciding the boundary of the usage context that should be taken into account because it is essentially difficult to decide which context element should be included as the system requirements. If a developer explores the context boundary in an ad-hoc manner, the developer will be faced with the *frame problem* because there are unlimited context elements in the real world where the target system exists. There are many application domains that should take into account the *frame problem*: security, safety, network threats, and user interactions. To deal with this problem, this paper proposes a new type of requirements analysis method for exploring the context boundary using guide words, a set of hint words for finding a context element affecting the system behavior. The target of our method is embedded systems that can be abstracted as a sensor-and-actuator machine exchanging the physical value between a system and its context. In our method, only the *value-context elements*, a kind of *value objects*, are extracted as the associated context elements. By applying the *guide words*, we can explore only a sequence of context elements affecting the data value and avoid falling into the *frame problem* at the requirements analysis phase.

Keywords: Context analysis, Frame problem, Embedded systems.

1 Introduction

Many embedded systems not only affect their context through actuators but also are affected by their context through sensors. The term *context* refers to the real world such as the usage environment that affects the system behavior.

In most cases, context is only roughly analyzed in comparison to functional or non-functional system requirements. As a result, unexpected behavior may emerge in a system if a developer does not recognize any possible conflicting combinations between the system and its context. It is also difficult to decide the boundary of the context that should be taken into account: which context element, an object existing outside of the system, should be included as the targets of requirements analysis. If a developer explores the context boundary in an ad-hoc manner, he or she will be faced with the *frame problem* [7] because there are unlimited context elements in the real world where the system exists. The

frame problem is the problem of representing the effects of the system behavior in logic without explicitly specifying a large number of conditions not affected by the behavior.

To deal with the *frame problem* in embedded systems, we propose CAMEmb (Context Analysis Method for Embedded systems), a context-dependent requirements analysis method. A context model is constructed from the initial system requirements by using the *UML Profile for Context Analysis*. This context model clarifies the relation between a system and its context. In CAMEmb, only the *value-context elements*, a kind of value objects, are extracted as the associated context elements because many embedded systems are abstracted as a sensor-and-actuator machine exchanging the physical value between a system and its context. Applying the *Guide Words for Context Analysis*, we can explore only a sequence of context elements directly or indirectly affecting the data value observed or controlled by the system sensors and actuators. Other context elements not affecting the system observation and control are not taken into account because these context elements do not affect the system behavior. We can deal with the *frame problem* because we only have to consider limited number of context elements as the context of the target system.

The remainder of this paper is structured as follows. In Section 2, problems in the current requirements analysis methods are pointed out in terms of the *frame problem*. In Section 3 and 4, CAMEmb is introduced to deal with the *frame problem*. In Section 5, we discuss on the relation between CAMEmb and the *problem frame approach* [5]. Moreover, we discuss how to apply our idea to other domains such as security. Concluding remarks are provided in Section 6.

2 Motivation

In this section, typical problems in the current requirements analysis methods are pointed out by describing the specification of an electric pot as an example.

2.1 Motivating Example

An electric pot is an embedded system for boiling water. Here, for simplicity, only the following is considered: 1) the pot has three hardware components: a heater, a thermostat, and a water level sensor; 2) the pot controls the water temperature by turning on or off the heater; 3) the pot changes its mode from the heating mode to the retaining mode when the temperature becomes 100 Celsius; and 4) the pot observes the volume from the water level sensor that detects whether water is below or above a certain base level.

In case of the electric pot, the water temperature should be taken into account as an important context element. Here, as an example, let us consider the specification that controls the water temperature. In most cases, this specification is described by implicitly taking into account the specific context—for example, such the context that water is boiled under the normal air pressure. A developer describes the software logic corresponding to the specific context—in

this case, the pot continues to turn on a heater switch until the water temperature becomes 100 Celsius. Below is the specification described in pseudo code. This function describes that a controller continues to turn on a heater while the value of the temperature obtained from a thermostat is below 100 Celsius. The `Boil` function behaves correctly under the normal circumstance.

```
// Boil function
while thermostat.GetTemperature() < 100.0
  do heater.On();
```

Although this traditional approach is effective, there is room for improvements because it does not explicitly consider the context elements such as water and air pressure. The above `Boil` specification looks correct. However, faults may occur if the expected context is changed—for example, the circumstance of the low air pressure. Because the boiling point is below 100 Celsius under this circumstance, the software controller continues to heat water even if its temperature becomes the boiling point. As a result, water evaporates and finally its volume will be empty. The water level sensor observes the volume, and the pot stops heating. Although this behavior satisfies the above system specification, the pot may be useless for the people who use it up on high mountains where the air pressure is low.

2.2 Problems to be tackled

The boundary of the context should be determined from stakeholders' requirements. If we consider climbers as customers of the pot, we have to admit that we failed in eliciting requirements in the above example.

It is not easy to define the context boundary even if the target users of the system are determined. A developer will be faced with the *frame problem* because there are unlimited context elements in the real world. There are some studies that take into account the real world as a modeling target. For example, Greenspan, S. et al. claim the necessity of introducing real world knowledge into requirement specifications [2]. But, current requirements elicitation methods do not answer a question: how and why do we find air pressure as a context element ? Of course, domain knowledge and past experiences are important to find this kind of requirements elicitation. Moreover, we admit that there are no complete methods to overcome the *frame problem*. However, at the same time, we need a method for systematically exploring the context boundary because many incidents that occur in the real embedded systems are caused by insufficient context analysis. That is, unexpected context influence that cannot be predicted in the requirements elicitation phase tends to cause a crucial incident. Many engineers in the industry face this problem.

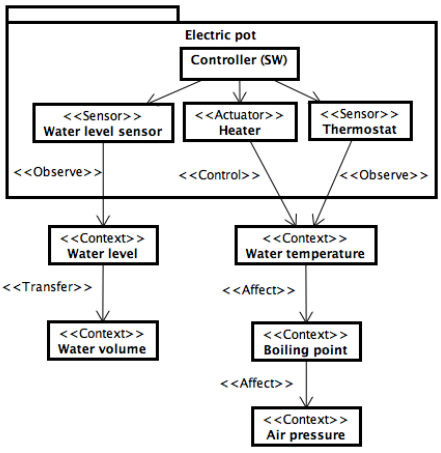

Fig. 1. Context analysis model for an electric pot

3 CAMEmb

CAMEmb is a context analysis method for dealing with the problem pointed out in Section 2. CAMEmb complements the insufficiency of the traditional requirements analysis methods.

3.1 Context analysis model

Figure 1 illustrates the result of context analysis for an electric pot. The upper side and the lower side show a system and its context, respectively. The details of the *Controller* in the context model are described in the system analysis model. Sensors and actuators for observing or controlling the context are regarded as the interface components that separate the context from a system. Figure 1 shows only the structural aspect of the context modeling. The details of the *Controller* and the behavioral aspect of the context model are omitted due to the space limitation. In CAMEmb, the behavioral aspect is modeled using state machine diagrams. The structural aspect plays an important role in exploring the context boundary as mentioned below.

3.2 UML profile for context analysis

A UML profile is provided for context analysis. This profile can describe system elements, context elements, and associations between them: four kinds of stereotypes including $\ll Context \gg$, $\ll Hardware \gg$, $\ll Sensor \gg$, and $\ll Actuator \gg$ are defined as an extension of the UML class ($\ll Sensor \gg$ and $\ll Actuator \gg$ are subtypes of $\ll Hardware \gg$); and five kinds of stereotypes including $\ll Observe \gg$, $\ll Control \gg$, $\ll Transfer \gg$, $\ll Affect \gg$, and

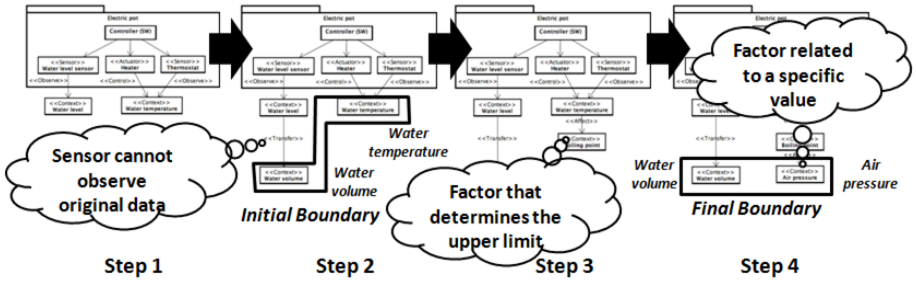

Fig. 2. Stepwise context analysis using guide words (for illustration only)

$\ll Noise \gg$ are defined as an extension of the UML association. The arrow of $\ll Observe \gg$ and $\ll Control \gg$ indicates the target of observation and control. The arrow of $\ll Noise \gg$ and $\ll Affect \gg$ indicates the source of noise and affect, respectively. The arrow of $\ll Transfer \gg$ indicates the source of transformation. The associations between *Controller* and three hardware components (sensors and actuators) indicate the phenomena such as *sending a command from software to hardware* and *receiving data from hardware*. However, stereotypes for these phenomena are not provided in our UML profile because they should be considered in system analysis not in context analysis.

4 Stepwise context analysis using guide words

The context model shown in Figure 1 is created as illustrated in Figure 2. Figure 2 shows only the image of context analysis procedures. Please refer to Figure 1 when a detailed analysis result is needed.

Step1: extract directly observed or controlled context elements

First, context elements ($\ll Context \gg$), which are directly observed or controlled by a sensor or an actuator, are extracted. We regard the environment value as a context element because CAMEmb focuses on embedded systems based on sensing and actuating. We call these context elements *"value-context elements"*. In case of an electric pot, *water level* and *water temperature* are extracted since *water level* is observed by the water level sensor and *water temperature* is controlled by the heater.

Step 2 [Initial boundary]: extract indirectly observed or controlled context elements

An element directly observed by a sensor may be an alternative context element in such a case that the sensor cannot observe the original value of the target context element. For example, the pot wants to observe not the *water level*

Table 1. Guide words for context analysis

No.	Category of $\ll Affect \gg$	Guide word
1.	physical phenomena	factor that determines the upper limit
2.	physical phenomena	factor that determines the lower limit
3.	physical phenomena	factor related to a specific value
4.	influence to sensing	factor that interferes with the observation
5.	influence to actuation	factor that interferes with the control

but the *water volume*. Next, we explore the target context elements by using $\ll Transfer \gg$. In the step 2, all paths from sensors and actuators to the target context elements are completely extracted. The initial context boundary is determined in this stage. In case of an electric pot, *water volume* and *water temperature* are extracted as the initial context boundary.

Step 3 [intermediate boundary]: extract impact factors using guide words

The initial context boundary is an ideal boundary in which system's sensing and controlling are not affected by other factors. However, there are many factors affecting observation and actuation in the real world. We have to extract these factors in order to develop reliable embedded systems.

In CAMEmb, impact factors that affect the states of these context elements are extracted using guide words. Guide words, hints for deriving related elements, are effective for software deviation analysis [6]. Guide words are mainly used in HAZOP (Hazard and Operability Studies). In HAZOP, deviation analysis is performed by using the guide words including *NOT*, *MORE*, *LESS*, *AS WELL AS*, *PART OF*, *REVERSE*, and *OTHER THAN*. For example, *higher pressure*, which may be deviated from a normal situation, can be derived from the property *pressure* and the guide word *high*.

In addition to the HAZOP guide words, CAMEmb provides a set of guide words specific to the context analysis as shown in Table 1. These guide words help us to find an obstacle that affects the system observation and control in terms of the *context-value*. By using these guide words, we can extract context elements that affect the context elements existing within the initial boundary. If there is a context element having the influence on another context element, we link them by the $\ll Affect \gg$ association.

In case of an electric pot, the *boiling point* can be extracted as an impact factor for the *water temperature* by applying the guide word *"factor that determines the upper limit"* since the temperature does not become higher than the boiling point. Step 3 in Figure 2 shows this stage of the context analysis.

4.1 Step 4 [Final boundary]: determine the context boundary

We have to continue to extract impact factors as many as possible to develop reliable systems. In case of an electric pot, the *air pressure* can be extracted as

an impact factor for the *boiling point* by applying the guide word *"factor related to a specific value"* since the boiling point of the water is 100 Celsius under the circumstance of 1.0 atm. At this point, we finish the context exploration because we can find no more impact factors affecting the *air pressure*.

We can extract two context elements *water volume* and *air pressure* as the final context boundary.

As shown here, the boundary of the context is explored by using *UML Profile for Context Analysis* and *Guide Words for Context Analysis*. We can explore only a sequence of context elements directly or indirectly affecting the data value observed or controlled by the system sensors and actuators. Other context elements not affecting the system observation and control are not extracted. There are many context elements such as person, table, and light in the environment of an electric pot. However, these context elements do not affect the data observed or controlled by the pot. So, we do not have to take into account these context elements. These context elements exist out of the boundary.

5 Discussion

5.1 Avoidance of the frame problem

In CAMEmb, we select only the elements affecting the data value observed or controlled by a system. We think that the value-based context analysis is reasonable because most embedded systems observe the input data from the environment through sensors and affect the environment by emitting the physical outputs through actuators. The system behavior is determined by the data observed by the sensors and controlled by the actuators. We have only to take into account the context elements explicitly or implicitly affecting the data linked with the $\ll Transfer \gg$ or the $\ll Affect \gg$ associations. The context analysis terminates when there are no more context elements affecting the data. In our approach, the affection is determined by using guide words. Of course, the method using guide words is not complete. But, the method helps a developer to find the context elements affecting the system behavior as many as possible.

5.2 Problem frames

Jackson, M. proposes the *problem frames approach* in which relations between a machine (a system to be developed) and the real world are explicitly described. The approach emphasises on the importance of analysing the real world and the problems. The notion of context in CAMEmb corresponds to the real world in the problem frame. Examples of formalising requirements with problem frames can be found in [1] [3]. We believe that CAMEmb provides a fruitful mechanism for using the *problem frames approach* more effectively. The *problem frames approach* is strong in analysing the real world (context) in terms of the problems. On the other hand, CAMEmb is strong in exploring the context boundary.

5.3 Application to other domains

Parnas, D. L. and Madey J. propose the *four-variable model* [8] in which the functions, timing, and correctness are described by using monitored variables, control variables, and input / output data items. The *four-variable model* was used to specify the requirements for the A-7 aircraft in SCR (Software Cost Reduction) [4] providing a tabular notation for specifying requirements. The *four-variable model* is similar to CAMEmb because monitored variables and control variables correspond to context elements observed by sensors and controlled by actuators.

Although we may not be able to apply CAMEmb to all the application domains, there are many domains that can be modelled as monitor-controller (or sensor-actuator) systems. Security, safety, network threats, and user interactions are examples of such domains. In these domains, context can be analyzed using our approach. For example, *trust* in the security domains correspond to *value* in CAMEmb. By defining the *guide words* that affect the trusts, we can explore the trust boundary.

6 Conclusion

In this paper, we proposed CAMEmb, a context-dependent requirements analysis method. As demonstrated in this paper, we could provide a method for exploring the context boundary. The idea of *value-context elements* and *guide words* plays an important role. We think that the essential idea of CAMEmb can be applied to other kinds of context such as security and safety in embedded systems. As the next step, we plan to apply CAMEmb to such an application.

References

1. Coleman, J. W. and Jones, C. B.: Examples of how to Determine the Specifications of Control Systems, In *Proceedings of Workshop on Rigorous Engineering of Fault-Tolerant Systems (REFT 2005)*, pp.65-73, 2005.
2. Greenspan, S., Mylopoulos, J., and Borgida, A.: Capturing More World Knowledge in the Requirements Specification, In *Proceedings of International Conference on Software Engineering (ICSE'82)*, pp.225-234, 1982.
3. Hayes, I., Jackson, M., and Jones, C.: Determining the specification of a control system from that of its environment, In *International Symposium for Formal Methods Europe (FME 2003)*, pp.154-169, 2003.
4. Heitmeyer, C. L., Bull, A., Gasarch, C., and Labaw, B. G. SCR*: A Toolset for Specifying and Analyzing Requirements, In *Proceedings of Computer Assurance (COMPASS)*, pp.109122, 1995.
5. Jackson, M: *Problem Frame: Analyzing and Structuring Software Development Problems*, Addison-Wesley, 2001.
6. Leveson, N. G.: *Safeware: System Safety and Computers*, Addison-Wesley Publishing Company, 1995
7. McCarthy, J. and Hayes, P. J.: Some Philosophical Problems from the Standpoint of Artificial Intelligence, *Machine Intelligence*, 4, pp.463-502, 1969.
8. Parnas, D. L. and Madey, J.: Functional Documentation for Computer Systems Engineering, *McMaster University, Technical Report CRL 237*, 1991.