Specifying Optimal Design for a Steam-boiler System

Li XiaoShan
UNU/IIST, Macau
Wang JuAn
University of Macau

May 1996

Extended Abstract

A Mean Value Calculus, an interval based logic of time is applied in this paper to specify and verify the steam-boiler control problem for Dagstuhl seminar. In addition to specifying safety property, emphasis is put on capturing non-functional requirements which reflect the qualities of designs, such as performance and optimization. From the case study, we present a general methodology of specifying and verifying this kind of sampling control systems. That is, firstly giving the specification of the mathematical model of the physical plant; then presenting the specification for the mathematical model of the sampling system; thirdly making design decisions by analyzing the mathematical models and requirements; finally verifying the design satisfying the requirements of the system.

Hybrid systems contain both continuous and discrete variables of time. Generally, only physical plants of an automatic control system contain continuous variables, and the variables in decision makers, i.e., the computer control programs are discrete. Plant and decision maker are connected by the sensors and actuators. Computer control programs in decision makers first obtain sampling data from sensors before making control decisions. The plant is controlled through actuators while it provides feedback to controlling programs via sensors.

A steam-boiler control problem was provided in J.-R. Abrial as a testing case for the existing formal methods. It represents a typical hybrid system which is a challenge for formalization. In order to provide a concise solution, the original problem is simplified. The system comprises the following main units: a boiler, a sensor of water, one pump, one pump controller, a sensor of pump, and a sensor of steam.

The total capacity of the steam-boiler is C liters. There are two dangerous bounds for the water quantity in the steam-boiler: the minimal limit M_1 (in

liters) and maximal limit M_2. When the water quantity, denoted by a continuous variable q, is below M_1 or above M_2 after five seconds, the system will be in danger. This is the safety requirement of the system.

There are also two normal water quantity bounds N_1 and N_2. The preferable water quantity ($N_1 < q < N_2$) should be maintained during regular operation. This is a performance requirement for the system.

For simplification, it is assumed that the pump can supply water immediately when it is opened. The throughput of the pump, denoted by p (in liters/sec), can be adjusted from 0 (i.e. , the pump is closed) to its maximal capacity P (in liters/sec). The general cases of this problem with four pumps and delays are discussed in the paper.

The control program communicates with the physical units (plant, sensors and actuators) through message passing. A sampling event occurs every five seconds. When it happens, the program first receive messages from the physical units, i.e., getting the values of q, v(steam output), and two Boolean states R(representing the system is running) and S(representing the water sensor works well). Then the control program analyzes the information and calculate the suitable pump control value p by the control decisions. Finally, the control value p is transmitted to the physical pump by the controller.

The time for message transmission is assumed to be zero.

The system behavior can be characterized by water quantity q, the steam output v and the throughput of the pump p. They are continuous functions of time. The mathematical model of physical plant can be established through the following laws in MVC:

$\Box\lceil 0 \leq q < C \rceil^*$ (Law_1)

$\Box\lceil 0 \leq p \leq P \rceil^*$ (Law_2)

$\Box\lceil 0 \leq v \leq W < P \rceil^*$ (Law_3)

$\Box\lceil -U_2 \leq \dot{v} \leq U_1 \rceil^*$ (Law_4)

$\Box\lceil \dot{q} = p - v \rceil^*$ (Law_5)

Since the program follows a cycle which takes place every five seconds to sample data and make decisions, a mathematical model for sampling is needed to capture the requirements formally. We use $\bar{q}$, $\bar{v}$ and $\bar{p}$ to characterize sampling data in control program. which are piece-wise continuous functions and are assumed to be right continuous.

The events are introduced for the model, which are δ-functions (only to be 1 at isolated time points) in MVC. sp represents the sampling event. Event $\uparrow R$ starts the steam-boiler. Event $\downarrow R$ stops the steam-boiler and event $\downarrow S$ means the water sensor is broken at sampling time.

The sampling behavior can be formalized by the following sampling law.

$\Box((\lceil R \rceil \wedge (l = 5) \Rightarrow \Diamond sp) \wedge (sp; \lceil \neg sp \wedge R \rceil; sp \Rightarrow l = 5))$ (Law_6)

It means a sampling event occurs in every five seconds during the system operation and there are exact five seconds between two adjacent samplings.

When the system works perfectly, the water sensor provides correct water quantity at sampling points. As we assume that the steam and pump sensors

always work properly, they provide correct information in any cases.

$\Box(\lceil S\rceil^0 \wedge sp \Rightarrow \lceil \bar{q} = q\rceil^0)$ (Law_7)

$\Box(sp \Rightarrow \lceil \bar{v} = v\rceil^0 \wedge \lceil \bar{p} = p\rceil^0)$ (Law_8)

Since the pump is controlled by the decision maker(program), we always have

$\Box(\bar{p} = p)$ (Law_9)

If the water sensor is broken down, the water quantity is estimated by the following calculation:

$sp \wedge \lceil \bar{q} = a_0 \wedge \bar{p} = b_0\rceil^0; l = 5; sp \wedge \lceil \neg S\rceil^0 \Rightarrow l = 5; \lceil \bar{q} = a_0 + 5b_0 - \widehat{\int v}\rceil^0 (Law_{10})$

where $\widehat{\int v}$ is the estimation of $\int v$, which is the steam quantity emitted from the steam-boiler within one sampling cycle. It is a function of the two sampling steam values in a sample cycle. The value of $\widehat{\int v}$ in a sample cycle depends on the concrete situation of steam-boiler. The analysis and calculation of $\widehat{\int v}$ is discussed in the paper. Law_{10} is derived from Law_5. If the water sensor works well, $\int v$ can be calculated precisely by Law_5.

For simplification, we make some assumptions about the system. For example,

$\uparrow R \Rightarrow \lceil M_1 < q < M_2\rceil^0 \wedge \lceil S\rceil^0$ $(Assum_5)$

$Assum_5$ assumes that the system starts with its water quantity q within the safe range $[M_1, M_2]$ and the water sensor works well at the beginning.

We use Law and $Assum$ to represents all laws and assumptions about the system hereafter.

$Law_1 \wedge Law_2 \wedge \cdots \wedge Law_{10}$ (Law)

$Assum_1 \wedge Assum_2 \wedge \cdots \wedge Assum_7$ $(Assum)$

The reasonable design of the steam-boiler system should satisfy the following requirements from the discussion above.

Safety The water quantity q in the steam-boiler can never exceed continuously the safe bounds for more than 5 seconds.

$\Box(((\lceil q < M_1\rceil \wedge \lceil R\rceil) \Rightarrow l \leq 5) \wedge ((\lceil q > M_2\rceil \wedge \lceil R\rceil) \Rightarrow l \leq 5))$ **(Req)**

This is the basic requirement for the system since any design must guarantee it. For simplification without loosing generality, the safety requirement (Req) is changed into the sampling safety requirement $(Safe)$ as follows

$sp \wedge \lceil R\rceil^0 \Rightarrow \lceil M_1 < q < M_2\rceil^0$ **(Safe)**

It means that at each sampling time we must guarantee the quantity of water q in the safe range $[M_1, M_2]$ while the system is running. Obviously, it implies the safety (Req). Meanwhile it also implies that the event $\downarrow R$ must occur when q is in the safe range $[M_1, M_2]$, i.e., $sp \wedge (\lceil q \leq M_1\rceil^0 \vee \lceil q \geq M_2\rceil^0) \Rightarrow \downarrow R$.

Performance If the water sensor works perfectly, the whole system should not be stopped and the water quantity should be kept within normal bounds continuously and stably.

$$\Box(\lceil N_1 + 5W < q < N_2 - 5P\rceil^0; \lceil S \wedge R\rceil) \Rightarrow \lceil N_1 < q < N_2\rceil) \qquad \textbf{(Perf)}$$

A better design should have this good performance property.

Optimization If the water sensor is broken down, the whole system should not be stopped until it has to. In other words, the rescue time should be as long as possible.

$$\Box(\downarrow S; \lceil \neg S \wedge R\rceil; \downarrow R \Rightarrow l \geq 5(m+1)) \qquad \textbf{(Opt)}$$

in which $m = min\{n \mid (\sum_{i=1}^{n} S_{\Box}^{i} + S_{\triangle}^{n+1}) \geq (M_2 - M_1)\}$, and

$S_{\Box}^{i} = [25U_1U_2 + 5(U_1 - U_2)(v_i - v_{i-1}) - (v_i - v_{i-1})^2]/(U_1 + U_2)$ and

$S_{\triangle}^{n+1} = 25(U_1 + U_2)/2$.

If a design satisfies this optimal property, it is one of the optimal designs for the steam-boiler system. The details of parameters in the above formulas can be referred to the paper.

After formally specifing the mathematical model and requirements of the system, we should give a reasonable design, i.e., a group of decisions in control program. This is the main work for a system design. Generally, a formal method should specify the design procedure formally and can prove that the design satisfies the requirements of the system by the formal proof system.

Performance decisions When the water sensor works properly, the design should guarantee that the water quantity stays in the normal range $[N_1, N_2]$. The following two control decisions are used to control the pump while the water sensor works properly:

$$sp \wedge \lceil R \wedge S\rceil^0 \wedge \lceil q < K_1\rceil^0 \Rightarrow \lceil p = P\rceil^0 \qquad \textbf{(Des}_\textbf{1}\textbf{)}$$
$$sp \wedge \lceil R \wedge S\rceil^0 \wedge \lceil q > K_2\rceil^0 \Rightarrow \lceil p = 0\rceil^0 \qquad \textbf{(Des}_\textbf{2}\textbf{)}$$
$$\lceil p = a\rceil; sp \wedge \lceil R \wedge S\rceil^0 \wedge \lceil K_1 \leq q \leq K_2\rceil^0 \Rightarrow (l > 0); \lceil p = a\rceil^0 \qquad \textbf{(Des}_\textbf{3}\textbf{)}$$

where $K_1 = N_1 + 5W$, $K_2 = N_2 - 5P$ and $a \in \{0, P\}$.

Des_1 is to open the pump at maximal quantity $p = P$ if the system is in the situation of $\lceil R \wedge S\rceil^0 \wedge \lceil q < K_1\rceil^0$ at sampling time. Similarly, if $\lceil R \wedge S\rceil^0 \wedge \lceil q > K_2\rceil^0$ holds at sampling time , the pump will be closed by Des_2. Des_3 is to keep the pump as before if $\lceil R \wedge S\rceil^0 \wedge \lceil K_1 \leq q \leq K_2\rceil^0$ holds at sampling time.

By the decisions above, the steam-boiler system can be verified to satisfy the performance requirement $(Perf)$ when the water sensor works well.

Theorem 1

$Assum \wedge Law \wedge Des_1 \wedge Des_2 \wedge Des_3 \Rightarrow Perf$

Rescue decisions When the water sensor is broken down, we should control the system as long as possible by estimating the water quantity q in the steam-boiler. We only shut down the system when we can not guarantee the value of

q is in the safe range $[M_1, M_2]$. This is the fault tolerant requirement to the system design. For the steam-boiler system, if one correct design has a longer rescue time while the water sensor is broken down, it is better. By analysing the system model, we find there exists an optimal rescue time limit, which gives an optimal design. The interesting resultis that we find are two optimal control conditions.

One is the controllable condition (CC)

$$\lceil R \wedge \neg S \rceil^0 \wedge \lceil x + y > S_\triangle \rceil^0 \wedge \lceil (x > 0) \wedge (y > 0) \rceil^0 \qquad (\mathbf{CC})$$

where $x = M_2 - qa2$ and $y = qa1 - M_1$.

If the condition (CC) holds at the sampling time, then the system is controllable by opening the pump properly. Otherwise, the steam-boiler is not controllable, that is to say, the water quantity q may be out of the safe range $[M_1, M_2]$, and we can find it at next sampling time. If so we stop the system.

The other is the pump control condition (PC)

$$max\{0, (S_{max} - y)\} \leq 5p \leq min\{5P, (S_{min} + x)\} \qquad (\mathbf{PC})$$

This condition requires that the pump must be open in the suitable range. Otherwise the water quantity q may be out of the safe range $[M_1, M_2]$ by the fault control.

Details of the parameters in above formulas can be referred to the complete paper.

According to (CC) and (PC), we give the following rescue decisions :

$$CC \wedge sp \wedge \lceil (x > S_\triangle) \wedge (x \geq y) \rceil^0 \Rightarrow \lceil p = S_{max}/5 \rceil^0 \qquad (\mathbf{Des_4})$$
$$CC \wedge sp \wedge \lceil (y > S_\triangle) \wedge (y > x) \rceil^0 \Rightarrow \lceil p = S_{min}/5 \rceil^0 \qquad (\mathbf{Des_5})$$
$$\lceil R \wedge \neg S \rceil^0 \wedge sp \wedge \lceil (0 < x < S_\triangle) \wedge (0 < y < S_\triangle) \rceil^0 \Rightarrow \lceil p = (2S_{min} + S_\triangle + x - y)/10 \rceil^0 \qquad (\mathbf{Des_6})$$
$$\lceil R \wedge \neg S \rceil^0 \wedge sp \wedge \lceil (x \leq 0) \vee (y \leq 0) \rceil^0 \Rightarrow \downarrow R \qquad (\mathbf{Des_7})$$

So we can prove the following theorems by the proof system of MVC.

Theorem 2
$Assum \wedge Law \wedge Des_4 \wedge Des_5 \wedge Des_6 \wedge Des_7 \Rightarrow Opt$

Theorem 3
$Assum \wedge Law \wedge Des_1 \wedge Des_2 \wedge Des_3 \wedge Des_4 \wedge Des_5 \wedge Des_6 \wedge Des_7 \Rightarrow Req$

In section of discussion and conclusion of the paper, we discussed some possible variants of the steam-boiler and compared with other contributions. Optimization is an interesting topic not only for control theory and engineering but also for computer science and engineering.

Evaluation and Comparison

1. Which parts of the system are specified at which level and in which way? (verbally, rigorously, formally?)

All parts of the system are specified formally. Particulaly, we presented the optimal design while the water sensor was broken down.

2.a. Does the solution comprise an implementation of a control program?

b. Has the control program been linked to the FZI simulator?

c. Has some experimentation been done with the control program?

No. However, the decisions of design are operational and it is not difficult to transform them into an implementation of a control program.

3. What are the comparable other solutions and what are the major differences wrt them? What other solutions complement the given solution and in which respect?

The paper deeply discusses the fault tolerant optimal design to the water sensor. The details on the communication, testing defaults of system and other problems we omitted can refer RS, CW1, VH and other contributions.

4. a. How much time has been spent on producing the solution? Give the number of person months, if possible for the various parts of the solution.

4 person months.

b. How much preparation is needed to become sufficiently expert of the used specification framework in order to be able to produce a solution to such a problem in that framework? Indicate the number of weeks of training which you believe is needed for an average programmer to learn the method.

4 weeks.

5. What are the premises for a good understanding of the proposed solution?

a. Is a detailed knowledge of the used formalism needed?

Yes.

b. Can an everage programmer understand the solution?

No.

c. How much time do you believe is necessary for the average programmer whithout knowledge of the used specification method to learn what is needed to be able to understand the solution?

4 hours.