# Testing Against Requirements Using UML Environment Models

Maritta Heisel[1] Denis Hatebur[1,2] Thomas Santen[3] Dirk Seifert[4]

[1]University Duisburg-Essen, Working Group Software Engineering,
{maritta.heisel,denis.hatebur}@uni-duisburg-essen.de
[2]Institut für technische Systeme GmbH, d.hatebur@itesys.de
[3]Technische Universität Berlin, Fachgebiet Softwaretechnik, santen@cs.tu-berlin.de
[4]Loria – Université Nancy 2, Équipe Dedale, dirk.seifert@loria.fr

## Abstract

We propose a new method for system validation by means of testing, which is based on environment models expressed as UML state machines. A sun blind control case study serves to illustrate the method. This article is an abbreviated version of [4].

## 1 Introduction

Model-based software development proceeds by setting up *models* of the software to be constructed. This approach has proven useful, because it allows developers to first elaborate the most important properties of the software before proceeding with the implementation. Often, software models are also used for code generation. In this case, however, a problem arises: it does not make sense any more to test the software against its models, because these were already used to generate it. We therefore propose to test the software not only against its *specification* (i.e., against the models), but also against its *requirements*, which describe the how the *environment* should behave in which the software will be operating (acceptance testing). For this purpose, we have to set up a model of the environment, too.

In this paper, we describe how UML state machines (with a corresponding support tool Teager) can be used to realize the described approach in the area of reactive and/or embedded systems. For this kind of system, state machine models are particularly useful. We elaborate on two different testing approaches: **On-the-fly testing:** Here, generating and executing test cases is intertwined. This has the advantage that state explosion is not a problem, but the disadvantage that for non-deterministic systems the tests may not be repeatable. **Batch testing:** Here, test cases are generated and stored for later execution. This has the advantage that regression tests can be performed more simply but the disadvantage that all possible behavior variants must be computed.

## 2 Terminology

Jackson's [5] terminology serves to clearly distinguish the different notions that have to be taken into account when developing software:

**Machine** is the thing we are going to build; it may consist of software and hardware.

**Environment** is the part of the real world where the machine will be integrated.

**System** consists of the machine *and* its environment.

**Requirements** are *optative* statements; they describe how the *system* should behave when the machine is in action.

**Specifications** are *implementable* requirements; they describe the behavior of the machine at its external interfaces and form the basis for its construction.

**Domain knowledge** is needed to transform requirements into specifications. It is expressed as *indicative* statements. We distinguish between facts and assumptions: **Facts** describe what holds in the environment, no matter how we build the machine. **Assumptions** describe things that cannot always be guaranteed, but which are needed to fulfill the requirements (e.g., rules for user behavior).

The domain knowledge $D$ consists of both the facts $F$ and the assumptions $A$: $D \equiv F \wedge A$. The relation between requirements and specifications is $S \wedge D \Rightarrow R$ (i.e., we have to show that if we build the machine such that it satisfies the specification $S$ and integrate it into an environment for which $D$ holds, then the requirements $R$ are satisfied).

## 3 Example

We illustrate our testing approach with the example of a sunblind control system. The task is to write software that controls a sunblind, taking into account user commands, wind, and sunshine: *The sunblind can manually be lowered or pulled up. It is automatically lowered on sunshine for more than one minute. The sunblind can be destroyed by heavy wind, which should be avoided. The environment consists of user, sun and wind.*

To illustrate the difference between requirements and specifications and to stress the importance of explicitly modeling the environment, we transform one

requirement concerning the sunblind control problem into a specification, making use of domain knowledge:

***R1*** *The sunblind is not destroyed by wind.*

To make this requirement implementable, we must know when wind can destroy the sunblind, and how a destruction can be avoided:

***F1*** *Heavy wind for more than 30 sec is destructive.*

***A1*** *Heavy wind for less than 30 sec is not destructive.*

***F2*** *If the sunblind is up, it cannot be destroyed by wind.*

Using this domain knowledge, we can replace $R1$ by:

***R1'*** *The sunblind is up if there is heavy wind for more than 30 sec.*

because $F1 \wedge \ A1 \wedge F2 \wedge R1' \Rightarrow R1$. Next, we use

***F3*** *It takes less than 30 sec to pull up the sunblind.*

to obtain

***R1"*** *If there is heavy wind and the sunblind is not up, it is pulled up.*

because $F3 \wedge R1'' \Rightarrow R1'$. Using the facts

***F4*** *There is heavy wind if and only if the wind sensor generates more than 75 pulses per sec.*

***F5*** *Turning the motor left pulls up the sunblind.*

we finally obtain the specification

***S1*** *If the wind sensor generates more than 75 pulses per sec and the last signals to the motor have not been* turn left*, followed by* motor left blocked *and* stop motor*, then the* turn left *signal is sent to the motor.*

(because $F4 \wedge F5 \wedge S1 \Rightarrow R1''$), which is quite different from the requirement we started out with. All in all, we have shown $F1 \wedge F2 \wedge F3 \wedge F4 \wedge F5 \wedge A1 \wedge S1 \Rightarrow R1$.

## 4 Test approach

How would the sunblind control software (SUT, system under test) be tested? Usually, conformance with the specification would be checked. In our example, we would have to verify that the machine generates the *turn left* signal. However, if the specification was not correctly derived from the requirements, the SUT would pass the test nevertheless. We therefore propose to test the SUT against the requirements. This means that we check whether the sunblind can enter a state where it would be destroyed. Besides detecting errors made in transforming requirements into specifications, testing against requirements allows us to verify that customer needs are satisfied (acceptance test).

In order to test the SUT against its requirements, we need a model of the environment, because the requirements refer to the environment and not to the machine. Much like the SUT, the environment can be modeled using UML state machines. The model explicitly contains the facts and the assumptions about the environment. The environment model consists of adapters and the input event generator: Adapters transform abstract events such as *pull up sun blind* into concrete ones, such as *turn motor left*. The input event generator produces abstract events. To capture stochastic properties of the environment probabilistic state machines of TEAGER can be used. This reduces

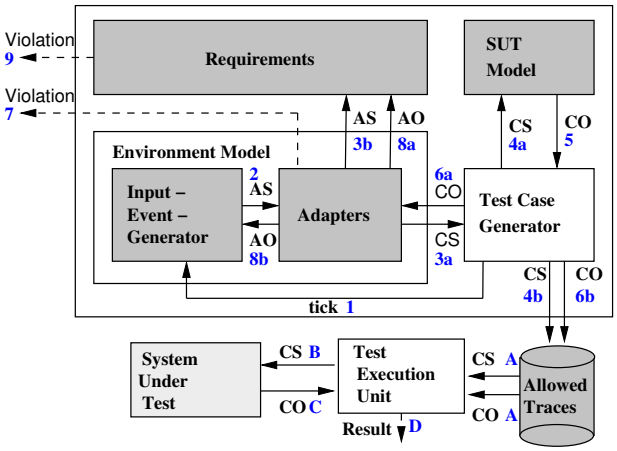


Figure 1: Test architecture for batch testing.

the number of inadequate test cases.

The requirements are translated into state machines, too. These state machines serve to inform the tester whether a requirement is violated. They observe the stimuli and SUT outputs at an adequate level of abstraction. As shown in Fig. 1, the Test Case Generator component of the tool TEAGER can be used to simulate the environment model and to check the requirements. To calculate test cases, for each tick (1) an abstract stimulus (2) is generated by the Input-Event-Generator in the environment model. Adapters transform the abstract stimuli into concrete stimuli for the Test Case Generator (3a) and send the abstract stimuli to the Requirements (3b). The Test Case Generator sends the concrete stimuli to the SUT Model (4a), which determines suitable responses (5), and it stores the concrete stimuli (4b) and the determined concrete observations (6b). The Adapters transform the concrete observations (6a) into abstract observations that are checked by the Requirements (8a) and used to generate reasonable stimuli (8b, e.g., *isLowered* only after *LoweredSunBlind*). Violations can be detected by checking the requirements (9) and while transforming concrete observations into abstract ones (7). After the requirements are checked, a new tick (1) is generated. The generated Test Cases can be used to test the SUT with the Test Execution Unit. Concrete stimuli and observations in the allowed traces (A) are used to stimulate the SUT (B) and check the responses (C). Test results (D) are the output of the Test Execution Unit.

Alternatively, the environment model can be directly connected to the SUT, and within the simulated environment the requirements are checked at runtime. In this case no SUT model is necessary. This scenario is especially useful for acceptance tests. The test system architecture – annotated with sample observations and stimuli for the sunblind example and with the execution order – for this "on the fly"-testing approach is shown in Fig. 2.

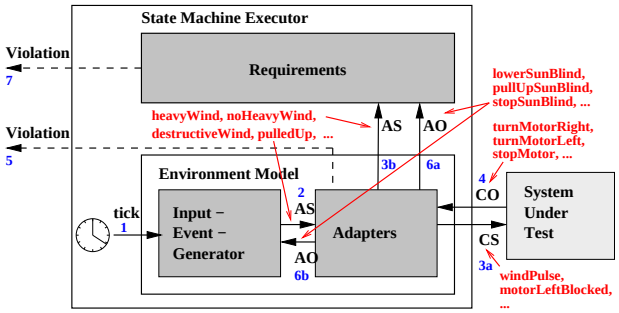


Figure 2: Test architecture for on-the-fly testing.

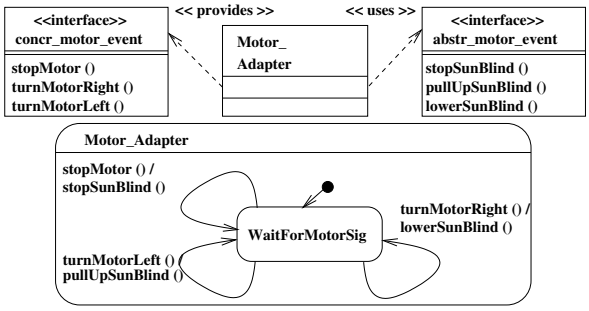


Figure 4: Adapter for the sunblind.

## 5 Patterns for environment models

Setting up the state machines for the environment model is not a trivial task. However, we can identify different patterns for setting up environment models, especially for expressing requirements as state machines. The overall structure of the state machine consists of parallel regions. That is, the environment model is in all of the parallel machines $R_i$, *Input-Event-Generator* and *Adapter* at the same time, and the different sub-machines communicate with each other via common events. Figure 3 shows an example of an input event generator. Note that assumption *A1* (namely, that heavy wind for less than 30 sec is not destructive) is modeled explicitly. Moreover, probabilities for the different transitions are given. These can be processed by the TEAGER tool. As an example of an adapter, we present the motor adapter, which transforms concrete observations into abstract ones (Fig. 4). It specifies how motor commands correspond to events that are visible in the environment.

For modeling requirements, we have developed different patterns, of which we can present only one for reasons of space. The pattern is usable when the requirement has the form "When [$eventR_i$] happens, [controlled domain] should be in [$desiredStateR_i$]". Its representation as a state machine is shown in Fig. 5. When the event of interest happens, then the precondition of the requirement is fulfilled, and the event $checkR_i$ is generated. The state machine representing the postcondition contains the desired state and may also contain other states. Only if it is in the desired state, the test passes; otherwise, a violation is determined, or the test is inconclusive. The latter happens, for example, if the actual state of the system is not known. Then, the result of checking a requirement should neither be pass nor fail. In our example, we do not initially know the (physical) state of the sunblind. Hence, we introduce an "unknown state" (denoted by "?") expressing this situation (Fig. 3). Checking requirement $R_1$ in this state yields an inconclusive result. Requirement $R_1$ of Sect. 3 is an instance of this pattern: whenever there is destructive wind, the sunblind must be up. Figure 6 shows the instantiated pattern. Whenever the event *destructive Wind* occurs, the event *checkR1* is generated. If the sunblind is in state *up*, the requirement is satisfied. Otherwise, it is violated. The *Fail* state corresponds to a state where the sunblind would be destroyed.

All in all, to completely model the sunblind control problem, 4 input event generators, 4 adapters, and 7 requirement state machines have to be set up. All the requirements are instances of patterns.

## 6 Discussion

We have developed a novel approach to testing reactive and embedded systems, based on environment models and using UML state machines. To evaluate our approach, we used the TEAGER tool suite [6, 7]. It allows its users to generate and execute test cases or to directly stimulate the SUT. TEAGER logs the stim-

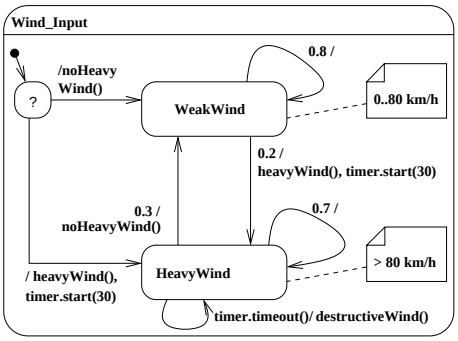


Figure 3: Input generator for the sunblind.

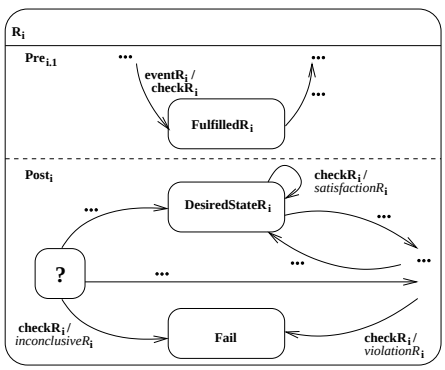


Figure 5: Patterns for environment models.

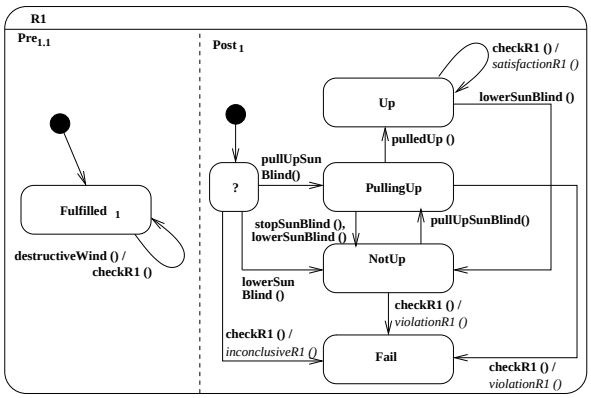


Figure 6: State machine for requirement $R_1$.

uli it sends to the SUT and the reactions of the SUT. During execution, these reactions are compared to the pre-calculated possible correct reactions to evaluate the test execution process [8]. Using Jackson's terminology, we have defined uniform architectures and procedures for on-the-fly as well as batch testing that have the following characteristics:

- Requirements, facts, and assumptions are modeled explicitly.
- We have defined patterns for the different state machines: For requirements, a parallel state machine is set up for each precondition. When all preconditions are fulfilled, the postcondition is checked. Input generators and adapters also consist of parallel state machines, one for each item of the environment that generates stimuli or receives observations, respectively.
- Once these models have been set up manually (but systematically), the tests are performed automatically, using the tool TEAGER.

To our knowledge, there neither exist approaches for testing requirements expressed as UML state machines, nor approaches for combining conformance testing on unit testing level with testing requirements on acceptance testing level. A detailed overview of the fundamental literature for classical formal testing can be found in Brinksma's and Tretmans' annotated bibliography [3]. In contrast to our work, most approaches assume that a testing process can communicate synchronously with the system under test. Belli at al. (see [2] and the work cited there) base their testing methodology on a variant of state machines. In contrast to our approach, they do not test against requirements, but against a fault model that has to be set up explicitly. Moreover, they do not execute the state machines directly, but represent them as event sequence graphs. Auguston et al. [1] use environment models for test case generation. In contrast to our approach, they do not use state machines, but attributed event grammars.

While these works have their merits, we think that the combination of environment models and UML state machines for testing is a particularly attractive one. Our approach has the following advantages: When **requirements change**, in the test case generator only the state machine describing those requirements must be changed. On the other hand, changed requirements will lead to a new SUT model. The new SUT model can be validated while the test cases are generated. Modeling the facts and assumptions about the environment supports the **validation of requirements**. For example, it can be discussed if heavy wind can be destructive to the sunblind within the time that a sunblind needs to be pulled up. Although the model of the environment has nearly the same complexity as the model of the machine, a structured approach to develop the environment model helps to **identify subproblems** that can be treated separately. Sometimes, states like "sunblind destroyed" are not modeled in the machine, but must be modeled in the environment to verify that this state cannot be reached. On the other hand, states can be left out in the environment model if the machine implements features that are not part of the requirements. The same environment model can be **(re-)used** for a sunblind control that can stop at an arbitrary height and a sunblind control that can only open or close the sunblind completely. Modeling the environment adds **diversity** to the development process and thus helps to avoid that the same mistake occurs for test development and SUT development. This is because the test developers, who model the environment, must think in terms of the environment rather than the SUT behavior. In the environment model, a reasonable test case selection strategy can be defined, so that **no inadequate test cases** are generated. Atypical behavior can be identified and tested using a dedicated environment model.

## References

[1] M. Auguston, J. B. Michael, and M.-T. Shing. Environment Behavior Models for Scenario Generation and Testing Automation. In *Workshop on Advances in Model-Based Testing (ICSE 2005)*, pages 1–6. ACM, 2005.

[2] F. Belli and A. Hollmann. Holistic testing with basic statecharts. In *Beiträge zu den Workshops (SE 2007)*, Lecture Notes in Informatics 106, pages 91–100. GI, 2007.

[3] E. Brinksma and J. Tretmans. Testing Transition Systems: An Annotated Bibliography. *LNCS*, pages 187–195, 2001.

[4] M. Heisel, D. Hartebur, T. Santen, and D. Seifert. Using UML Environment Models for Test Case Generation. In *Software Engineering 2008 - Workshopband*, Lecture Notes in Informatics. GI, 2008.

[5] M. Jackson. *Problem Frames. Analyzing & Structuring Software Development Problems.* Addison-Wesley, 2001.

[6] T. Santen and D. Seifert. Teager - Test Automation for UML State Machines. In *Software Engineering 2006*, Lecture Notes in Informatics P-79, pages 73–83. GI, 2006.

[7] D. Seifert. The TEAGER Tool Suite. Test Execution and Generation Framework for Reactive Systems. `swt.cs.tu-berlin.de/~seifert/teager.html`.

[8] D. Seifert. *Automatisiertes Testen asynchroner nichtdeterministischer Systeme mit Daten.* Shaker Verlag, 2007. Also: PhD dissertation, Technische Universität Berlin.