9

Pattern-driven Reuse of Behavioral Specifications in Embedded Control System Design

Miroslav Švéda, Ondřej Ryšavý & Radimir Vrba
Brno University of Technology
Czech Republic

1. Introduction

Methods and approaches in systems engineering are often based on the results of empirical observations or on individual success stories. Every real-world embedded system design stems from decisions based on an application domain knowledge that includes facts about some previous design practice. Evidently, such decisions relate to system architecture components, called in this paper as application patterns, which determine not only a required system behavior but also some presupposed implementation principles. Application patterns should respect those particular solutions that were successful in previous relevant design cases. While focused on the system architecture range that covers more than software components, the application patterns look in many features like well-known software object-oriented design concepts such as reusable patterns (Coad and Yourdon, 1990), design patterns (Gamma et al., 1995), and frameworks (Johnson, 1997). By the way, there are also other related concepts such as use cases (Jacobson, 1992), architectural styles (Shaw and Garlan, 1996), or templates (Turner, 1997), which could be utilized for the purpose of this paper instead of introducing a novel notion. Nevertheless, application patterns can structure behavioral specifications and, concurrently, they can support architectural components specification reuse.

Nowadays, industrial scale reusability frequently requires a knowledge-based support. Case-based reasoning (see e.g. Kolodner, 1993) can provide such a support. The method differs from other rather traditional procedures of Artificial Intelligence relying on case history: for a new problem, it strives for a similar old solution saved in a case library. Any case library serves as a knowledge base of a case-based reasoning system. The system acquires knowledge from old cases while learning can be achieved accumulating new cases. Solving a new case, the most similar old case is retrieved from the case library. The suggested solution of a new case is generated in conformity with the retrieved old case. This book chapter proposes not only how to represent a system's formal specification as an application pattern structure of specification fragments, but also how to measure similarity of formal specifications for retrieval. In this chapter, case-based reasoning support to reuse is focused on specifications by finite-state and timed automata, or by state and timed-state

sequences. The same principles can be applied for specifications by temporal and real-time logics.
The following sections of this chapter introduce the principles of design reuse applied by the way of application patterns. Then, employing application patterns fitting a class of real-time embedded systems, the kernel of this contribution presents two design projects: petrol pumping station dispenser controller and multiple lift control system. Via identification of the identical or similar application patterns in both design cases, this contribution proves the possibility to reuse substantial parts of formal specifications in a relevant sub-domain of embedded systems. The last part of the paper deals with knowledge-based support for this reuse process applying case-based reasoning paradigm.
The contribution provides principles of case-based reasoning support to reuse in frame of formal specification-based system design aiming at industrial applications domain. This book chapter stems from the paper (Sveda, Vrba and Rysavy, 2007) modified and extended by deploying temporal logic formulas for specifications.

2. State of the Art

To reuse an application pattern, whose implementation usually consists both of software and hardware components, it means to reuse its formal specification, development of which is very expensive and, consequently, worthwhile for reuse. This paper is aimed at behavioral specifications employing state or timed-state sequences, which correspond to Kripke style semantics of linear, discrete time temporal or real-time logics, and at their closed-form descriptions by finite-state or timed automata (Alur and Henzinger, 1992). Geppert and Roessler (2001) present a reuse-driven SDL design methodology that appears closely related approach to the problem discussed in this contribution.
Software design reuse belongs to highly published topics for almost 20 years, see namely Frakes and Kang (2005), but also Arora and Kulkarni (1998), Sutcliffe and Maiden (1998), Mili et al. (1997), Holzblatt et al. (1997), and Henninger (1997). Namely the state-dependent specification-based approach discussed by Zaremski et. al. (1997) and by van Lamsweerde and Wilmet (1998) inspired the application patterns handling presented in the current paper. To relate application patterns to the previously mentioned software oriented concepts more definitely, the inherited characteristics of the archetypal terminology, omitting namely their exclusive software orientation, can be restated as follows. A pattern describes a problem to be solved, a solution, and the context in which that solution works. Patterns are supposed to describe recurring solutions that have stood the test of time. Design patterns are the micro-architectural elements of frameworks. A framework -- which represents a generic application that allows creating different applications from an application sub-domain -- is an integrated set of patterns that can be reused. While each pattern describes a decision point in the development of an application, a pattern language is the organized collection of patterns for a particular application domain, and becomes an auxiliary method that guides the development process, see the pioneer work by Alexander (1977).
Application patterns correspond not only to design patterns but also to frameworks while respecting multi-layer hierarchical structures. Embodying domain knowledge, application patterns deal both with requirement and implementation specifications (Shaw and Garlan, 1996). In fact, a precise characterization of the way, in which implementation specifications

and requirements differ, depends on the precise location of the interface between an embedded system, which is to be implemented, and its environment, which generates requirements on system's services. However, there are no strict boundaries in between: both implementation specifications and requirements rely on designer's view, i.e. also on application patterns employed.
A design reuse process involves several necessary reuse tasks that can be grouped into two categories: supply-side and demand-side reuse (Sen, 1997). Supply-side reuse tasks include identification, creation, and classification of reusable artefacts. Demand-side reuse tasks include namely retrieval, adaptation, and storage of reusable artefacts. For the purpose of this paper, the reusable artefacts are represented by application patterns.
After introducing principles of the temporal logic deployed in the following specifications, next sections provide two case studies, based on implemented design projects, using application patterns that enable to discuss concrete examples of application patterns reusability.

3. Temporal Logic of Actions

Temporal Logic of Actions (TLA) is a variant of linear-time temporal logic. It was developed by Lamport (1994) primarily for specifying distributed algorithms, but several works shown that the area of application is much broader. The system of TLA+ extends TLA with data structures allowing for easier description of complex specification patterns.
TLA+ specifications are organized into modules. Modules can contain declarations, definitions, and assertions by means of logical formulas. The declarations consist of constants and variables. Constants can be uninterpreted until an automated verification procedure is used to verify the properties of the specification. Variables keep the state of the system, they can change in the system and the specification is expressed in terms of transition formulas that assert the values of the variables as observed in different states of the system that are related by the system transitions.
The overall specification is given by the temporal formula defined as a conjunction of the form

$$I \wedge \Box[N]_v \wedge L,$$

where I is the initial condition, N is the next-state relation (composed from transition formulas), and L is a conjunction of fairness properties, each concerning a disjunct of the next-state relation. Transition formulas, also called actions, are ordinary formulas of untyped first-order logic defined on a denumerable set of variables, partitioned into sets of flexible and rigid variables. Moreover, a set of primed flexible variables, in the form of v′, is defined. Transition formulas then can contain all these kinds of variables to express a relation between two consecutive states. The generation of a transition system for the purpose of model checking verification or for the simulation is governed by the enabled transition formulas. The formula $\Box[N]_v$ admits system transitions that leave a set of variables v unchanged. This is known as stuttering, which is a key concept of TLA that enables the refinement and compositional specifications. The initial condition and next-state relation specify the possible behaviour of the system. Fairness conditions strengthen the specification by asserting that given actions must occur.

The TLA+ does not formally distinguish between a system specification and a property. Both are expressed as formulas of temporal logic and connected by implication $S \Rightarrow F$, where S is a specification and F is a property. Confirming the validity of this implication stands for showing that the specification S has the property F.
The TLA+ is accompanied with a set of tools. One of such tool, the TLA+ model checker, TLC, is state-of-the-art model analyzer that can compute and explore the state space of finite instances of TLA+ models. The input to TLC consists of specification file describing the model and configuration file, which defines the finite-state instance of the model to be analysed. An execution of TLC produces a result that gives answer to the model correctness. In case of finding a problem, this is reported with a state-sequence demonstrating the trace in the model that leads to the problematic state. Inevitably, the TLC suffers the problem of state space explosion that is, nevertheless, partially addressed by a technique known as symmetry reduction allowing for verification of moderate size system specifications.

4. Petrol Dispenser Control System

The first case study pertains to a petrol pumping station dispenser with a distributed, multiple microcomputer counter/controller (for more details see Sveda, 1996). A dispenser controller is interconnected with its environment through an interface with volume meter (input), pump motor (output), main and by-pass valves (outputs) that enable full or throttled flow, release signal (input) generated by cashier, unhooked nozzle detection (input), product's unit price (input), and volume and price displays (outputs).

4.1 Two-level structure for dispenser control

The first employed application pattern stems from the two-level structure proposed by Xinyao et al. (1994): the higher level behaves as an event-driven component, and the lower level behaves as a set of real-time interconnected components. The behavior of the higher level component can be described by the following state sequences of a finite-state automaton with states "blocked-idle," "ready," "full fuel," "throttled" and "closed," and with inputs "release," (nozzle) "hung on/off," "close" (the preset or maximal displayable volume achieved), "throttle" (to slow down the flow to enable exact dosage) and "error":

blocked-idle $\xrightarrow{\text{release}}$ ready $\xrightarrow{\text{hung off}}$ full_fuel $\xrightarrow{\text{hung on}}$ blocked-idle
blocked-idle $\xrightarrow{\text{release}}$ ready $\xrightarrow{\text{hung off}}$ full_fuel $\xrightarrow{\text{throttle}}$ throttled $\xrightarrow{\text{hung on}}$ blocked-idle
blocked-idle $\xrightarrow{\text{release}}$ ready $\xrightarrow{\text{hung off}}$ full_fuel $\xrightarrow{\text{throttle}}$ throttled $\xrightarrow{\text{close}}$ closed $\xrightarrow{\text{hung on}}$ blocked-idle
blocked-idle $\xrightarrow{\text{error}}$ blocked-error
blocked-idle $\xrightarrow{\text{release}}$ ready $\xrightarrow{\text{error}}$ blocked-error
blocked-idle $\xrightarrow{\text{release}}$ ready $\xrightarrow{\text{hung off}}$ full_fuel $\xrightarrow{\text{error}}$ blocked-error
blocked-idle $\xrightarrow{\text{release}}$ ready $\xrightarrow{\text{hung off}}$ full_fuel $\xrightarrow{\text{throttle}}$ throttled $\xrightarrow{\text{error}}$ blocked-error

The states "full_fuel" and "throttled" appear to be hazardous from the viewpoint of unchecked flow because the motor is on and the liquid is under pressure -- the only nozzle valve controls an issue in this case. Also, the state "ready" tends to be hazardous: when the nozzle is unhooked, the system transfers to the state "full_fuel" with flow enabled. Hence, the accepted fail-stop conception necessitates the detected error management in the form of transition to the state "blocked-error." To initiate such a transition for flow blocking, the error detection in the hazardous states is necessary. On the other hand, the state "blocked-

idle" is safe because the input signal "release" can be masked out by the system that, when some failure is detected, performs the internal transition from "blocked-idle" to "blocked-error."

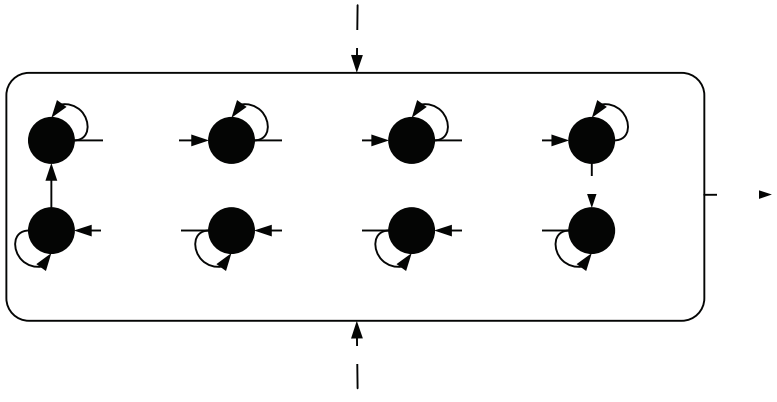

Fig. 1. Noise-tolerant impulse recognition automaton of length 8

4.2 Incremental measurement for flow control

The volume measurement and flow control represent the main functions of the hazardous states. The next applied application pattern, incremental measurement, means the recognition and counting of elementary volumes represented by rectangular impulses, which are generated by a photoelectric pulse generator. The maximal frequency of impulses and a pattern for their recognition depend on electro-magnetic interference characteristics. The lower-level application patterns are in this case a noise-tolerant impulse detector and a checking reversible counter. The first one represents a clock-timed impulse-recognition automaton that implements the periodic sampling of its input with values 0 and 1. This automaton with b states recognizes an impulse after b/2 (b>=4) samples with the value 1 followed by b/2 samples with the value 0, possibly interleaved by induced error values, see an example timed-state sequence:

$$(0, q_1) \overset{inp=0}{\rightarrow} \ldots \overset{inp=0}{\rightarrow} (i, q_1) \overset{inp=1}{\rightarrow} (i+1, q_2) \overset{inp=0}{\rightarrow} \ldots \overset{inp=0}{\rightarrow} (j, q_2) \ldots$$

$$\ldots \overset{inp=1}{\rightarrow} (k, q_{b/2+1}) \overset{inp=1}{\rightarrow} \ldots$$

$$\ldots \overset{inp=1}{\rightarrow} (m, q_{b-1}) \overset{inp=0}{\rightarrow} (m+1, q_b) \overset{inp=1}{\rightarrow} \ldots \overset{inp=1}{\rightarrow} (n, q_b) \overset{inp=0/IMP}{\rightarrow} (n+1, q_1)$$

i, j, k, m, n are integers representing discrete time instances in increasing order.

For the sake of fault-detection requirements, the incremental detector and transfer path are doubled. Consequently, the second, identical noise-tolerant impulse detector appears necessary.

The subsequent lower-level application pattern used provides a checking reversible counter, which starts with the value (h + l)/2 and increments or decrements that value according to

the "impulse detected" outputs from the first or the second recognition automaton. Overflow or underflow of the pre-set values of h or l indicates an error. Another counter that counts the recognized impulses from one of the recognition automata maintains the whole measured volume. The output of the letter automaton refines to two displays with local memories not only for the reason of robustness (they can be compared) but also for functional requirements (double-face stand). To guarantee the overall fault detection capability of the device, it is necessary also to consider checking the counter. This task can be maintained by an I/O watchdog application pattern that can compare input impulses from the photoelectric pulse generator and the changes of the total value; evidently, the appropriate automaton provides again reversible counting.
The noise-tolerant impulse detector was identified as a reusable design-pattern and its abstract specification written using TLA+ can be stored in a case library. This specification is shown in Fig. 2. The actions *Count1* and *Count0* capture the behaviour of the automaton at sampling times. Action *Restart* defines an output of the automaton, which is to pose the signal on *impuls* output as the signalization of successful impulse detection.

MODULE *ImpulseRecognition*

EXTENDS *Naturals*
CONSTANT B
ASSUME $B \in Nat \land B \geq 4$
VARIABLE $hold, input, impuls, b$

$TypeInvariant \triangleq b \in (1 \,..\, B+1) \land input \in \{0, 1\} \land impuls \in \{0, 1\} \land hold \in \text{BOOLEAN}$
$vars \triangleq \langle hold, input, impuls, b \rangle$

$Init \triangleq b = 1 \land input = 1 \land impuls \in \{0, 1\} \land hold = \text{FALSE}$

$Time \triangleq hold = \text{TRUE} \land hold' = \text{FALSE} \land \text{UNCHANGED } \langle input, impuls, b \rangle$

$Input \triangleq input' = 1 - input \land \text{UNCHANGED } \langle impuls, b, hold \rangle$

$Count1 \triangleq hold = \text{FALSE} \land b \in (1 \,..\, B \div 2) \land input = 1$
$\land \; b' = b + 1 \land hold' = \text{TRUE} \land \text{UNCHANGED } \langle input, impuls \rangle$

$Count0 \triangleq hold = \text{FALSE} \land b \in ((B \div 2) + 1 \,..\, B) \land input = 0$
$\land \; b' = b + 1 \land hold' = \text{TRUE} \land \text{UNCHANGED } \langle input, impuls \rangle$

$Restart \triangleq b = B + 1$
$\land \; b' = 1 \land impuls' = 1 - impuls \land \text{UNCHANGED } \langle input, hold \rangle$

$Next \triangleq Time \lor Input \lor Count1 \lor Count0 \lor Restart$

$Spec \triangleq Init \land \Box[Next]_{vars} \land \Box\Diamond(hold = \text{TRUE}) \land \text{WF}_{vars}(Time)$

THEOREM $Spec \Rightarrow \Box\, TypeInvariant$

Fig. 2.Abstract TLA specification of noise-tolerant impulse recognition automaton

4.3 Fault Maintenance Concepts

The methods used a ccomplish the fault management in the form of (a) hazardous state

reachability control and (b) hazardous state maintenance. In safe states, the lift cabins are fixed at any floors. The system is allowed to reach any hazardous state when all relevant processors successfully passed the start-up checks of inputs and monitored outputs and of appropriate communication status. The hazardous state maintenance includes operational checks and, for shaft controller, the fail-stop support by two watchdog processors performing consistency checking for both execution processors. To comply with safety-critical conception, all critical inputs and monitored outputs are doubled and compared; when the relevant signals differ, the respective lift is either forced (in case of need with the help of an substitute drive if the shaft controller is disconnected) to reach the nearest floor and to stay blocked, or (in the case of maintenance or fire brigade support) its services are partially restricted. The basic safety hard core includes mechanical, emergency brakes.
Because permanent blocking or too frequently repeated blocking is inappropriate, the final implementation must employ also fault avoidance techniques. The other reason for the fault avoidance application stems from the fact that only approximated fail-stop implementation is possible. Moreover, the above described configurations create only skeleton carrying common fault-tolerant techniques see e.g. (Maxion et al., 1987). In short, while auxiliary hardware components maintain supply-voltage levels, input signals filtering, and timing, the software techniques, namely time redundancy or skip-frame strategy, deal with non-critical inputs and outputs.

5. Multiple Lift Control System

The second case study deals with the multiple lift control system based on a dedicated multiprocessor architecture (for more details see Sveda, 1997). An incremental measurement device for position evaluation, and position and speed control of a lift cabin in a lift shaft can demonstrate reusability. The applied application pattern, incremental measurement, means in this case the recognition and counting of rectangular impulses that are generated by an electromagnetic or photoelectric sensor/impulse generator, which is fixed on the bottom of the lift cabin and which passes equidistant position marks while moving along the shaft. That device communicates with its environment through interfaces with impulse generator and drive controller. So, the first input, I, provides the values 0 or 1 that are altered with frequency equivalent to the cabin speed. The second input, D, provides the values "up," "down," or "idle." The output, P, provides the actual absolute position of the cabin in the shaft.

5.1 Two-level structure for lift control

The next employed application pattern is the two-level structure: the higher level behaves as an event-driven component, which behavior is roughly described by the state sequence

$$\text{initialization} \rightarrow \text{position\_indication} \rightarrow \text{fault\_indication}$$

and the lower level, which behaves as a set of real-time interconnected components. The specification of the lower level can be developed by refining the higher level state "position_indication" into three communicating lower level automata: two noise-tolerant impulse detectors and one checking reversible counter.

5.2 Incremental measurement for position and speed control

Intuitively, the first automaton models the noise-tolerant impulse detector in the same manner as in previous case, see the following timed-state sequence:

$$(0, q_1) \overset{inp=0}{\rightarrow} \ldots \overset{inp=0}{\rightarrow} (i, q_1) \overset{inp=1}{\rightarrow} (i+1, q_2) \overset{inp=0}{\rightarrow} \ldots \overset{inp=0}{\rightarrow} (j, q_2) \ldots$$

$$\ldots \overset{inp=1}{\rightarrow} (k, q_{b/2+1}) \overset{inp=1}{\rightarrow} \ldots$$

$$\ldots \overset{inp=1}{\rightarrow} (m, q_{b-1}) \overset{inp=0}{\rightarrow} (m+1, q_b) \overset{inp=1}{\rightarrow} \ldots \overset{inp=1}{\rightarrow} (n, q_b) \overset{inp=0/IMP}{\rightarrow} (n+1, q_1)$$

i, j, k, m, n are integers representing discrete time instances in increasing order.

The information about a detected impulse is sent to the counting automaton that can also access the indication of the cabin movement direction through the input D. For the sake of fault-detection requirements, the impulse generator and the impulse transfer path are doubled. Consequently, a second, identical noise-tolerant impulse detector appears necessary. The subsequent application pattern is the checking reversible counter, which starts with the value (h + l)/2 and increments or decrements the value according to the "impulse detected" outputs from the first or second recognition automaton. Overflow or underflow of the preset values of h or l indicates an error. This detection process sends a message about a detected impulse and the current direction to the counting automaton, which maintains the actual position in the shaft. To check the counter, an I/O watchdog application pattern employs again a reversible counter that can compare the impulses from the sensor/impulse generator and the changes of the total value.

The reuse of the noise-tolerant impulse detector is desirable. To do this, suitable patterns stored in a case library need to be identified. The method for identification of candidate patterns is based on the behavioural similarity by means of inclusion of a state sequence in models of stored specifications. The TLA tools can be used for formal checking whether a design pattern stored in a case library contains a state sequence that describes the new design. The new TLA module Query (see Fig. 3) is generated for the purpose of checking whether the design pattern from the previous case study can be reused in the multiple lift control system. Note that the formula is negated in order to get an example of concrete state-sequence in a model of matched specification. The state-sequence is shown in Fig. 4. It has 25 unique states and describes the behaviour that conforms to the required state-sequence defining the intended behaviour of noise-tolerant impulse detector for lift control system. In the reuse scenario, the required size of the new automaton is 4. The stored design pattern in a case library can be parameterized; hence the model-checking procedure instantiates the constant B = 4, which is defined in the accompanying configuration file.

MODULE *Query*

EXTENDS *ImpulseRecognition*

$$Trace \triangleq \neg((b = 1 \wedge input = 1) \rightsquigarrow (b = 2 \wedge input = 1) \rightsquigarrow (b = 3 \wedge input = 0) \rightsquigarrow (b = 4 \wedge input = 0) \rightsquigarrow b = 1)$$

Fig. 3. TLA Module Query containing sought-after timed-state sequence

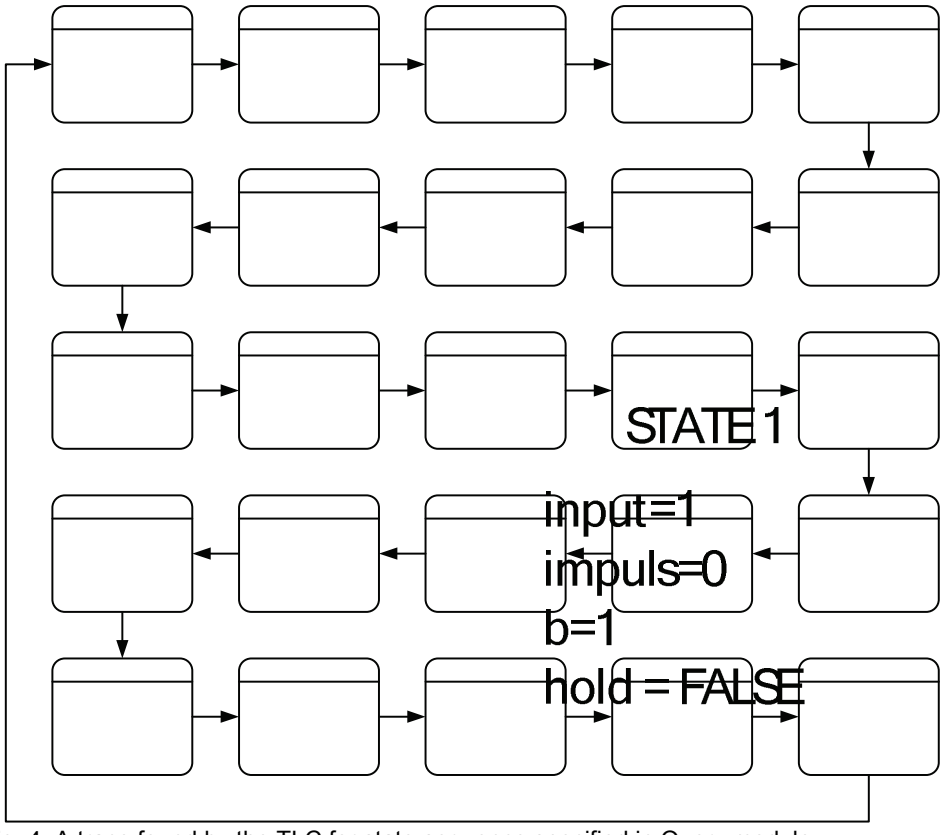

Fig. 4. A trace found by the TLC for state-sequence specified in Query module

5.3 Lift fault management

The approach used accomplishes a consequent application pattern, fault management based on fail-stop behavior approximations, both in the form of (a) hazardous state reachability control and (b) hazardous state maintenance. In safe states, the lift cabins are fixed at any floors. The system is allowed to reach any hazardous state when all relevant processors have successfully passed the start-up checks of inputs and monitored outputs and of appropriate communication status. The hazardous state maintenance includes operational checks and consistency checking for execution processors. To comply with safety-critical conception, all critical inputs and monitored outputs are doubled and compared. When the relevant signals differ, the respective lift is either forced (with the help of a substitute drive if the shaft controller is disconnected) to reach the nearest floor and to stay blocked.

The basic safety hard core includes mechanical, emergency brakes. Again, more detailed specification should reflect not only safety but also functionality with fault-tolerance support: also blocked lift is safe but useless. Hence, the above described configurations create only skeleton carrying common fault-tolerant techniques.

6. Application Patterns Reuse

The two case studies presented above demonstrate the possibility to reuse effectively substantial parts of the design dealing with petrol pumping station technology for a lift control technology project. While both cases belong to embedded control systems, their application domains and their technology principles differ: volume measurement and dosage control seems not too close to position measurement and control. Evidently, the similarity is observable by employment of application patterns hierarchy, see Table 1.

fault management based on fail-stop behavior approximations
two-level (event-driven/real-time) structure
incremental measurement
noise-tolerant impulse detector checking reversible counter /O watchdog

Table 1. Application patterns hierarchy.

The reused upper-layer application patterns presented include the automata-based descriptions of incremental measurement, two-level (event-driven/real-time) structure, and fault management stemming from fail-stop behavior approximations. The reused lower-layer application patterns are exemplified by the automata-based descriptions of noise-tolerant impulse detector, checking reversible counter, and I/O watchdog.
Clearly, while all introduced application patterns correspond to design patterns in the above-explained interpretation, the upper-layer application patterns can be related also to frameworks. Moreover, the presented collection of application patterns creates a base for a pattern language supporting reuse-oriented design process for real-time embedded systems.

7. Knowledge-Based Support

Industrial scale reusability requires a knowledge-based support, e.g. by case-based reasoning (see Kolodner, 1993), which differs from other rather traditional methods of Artificial Intelligence relying on case history. For a new problem, the case-based reasoning strives for a similar old solution. This old solution is chosen according to the correspondence of a new problem to some old problem that was successfully solved by this approach. Hence, previous significant cases are gathered and saved in a case library. Case-based reasoning stems from remembering a similar situation that worked in past. For software reuse, case-based reasoning utilization has been studied from several viewpoints as discussed e.g. by Henninger (1998), and by Soundarajan and Fridella (1998).

7.1 Case-Based Reasoning

The case-based reasoning method contains (1) elicitation, which means collecting those cases, and (2) implementation, which represents identification of important features for the case description consisting of values of those features. A case-based reasoning system can only be as good as its case library: only successful and sensibly selected old cases should be

stored in the case library. The description of a case should comprise the corresponding problem, solution of the problem, and any other information describing the context for which the solution can be reused. A feature-oriented approach is usually used for the case description.
Case library serves as the knowledge base of a case-based reasoning system. The system acquires knowledge from old cases while learning can be achieved accumulating new cases. While solving a new case, the most similar old case is retrieved from the case library. The suggested solution of the new case is generated in conformity with this retrieved old case. Search for the similar old case from the case library represents important operation of case-based reasoning paradigm.

7.2 Backing Techniques

Case-based reasoning relies on the idea that situations are mostly repeating during the life cycle of an applied system. Further, after some period, the most frequent situations can be identified and documented in the case library. So, the case library can usually cover common situations. However, it is impossible to start with case-based reasoning from the very beginning with an empty case library.
When relying on the case-based reasoning exclusively, also the opposite problem can be encountered: after some period the case library can become huge and very semi-redundant. Majority of registered cases represents clusters of very similar situations. Despite careful evaluation of cases before saving them in the case library, it is difficult to avoid this problem.
In an effort to solve these two problems, the case-base reasoning can be combined with some other paradigm to compensate these insufficiencies. Some level of rule-based support can partially cover these gaps with the help of rule-oriented knowledge; see (Sveda, Babka and Freeburn 1997). Rule-based reasoning should augment the case-based reasoning in the following situations:

- No suitable old solution can be found for a current situation in the case library and engineer hesitates about his own solution. So, rule-based module is activated. For a very restricted class of tasks, the rule-based module is capable to suggest its own solution. Once generated by this part of the framework, such a solution is then evaluated and tested more carefully. However, if the evaluation is positive, this case is later saved in the case library covering one of the gaps of the case-based module.
- Situations are similar but rarely identical. To fit closer the real situation, adaptation of the retrieved case is needed. The process of adaptation can be controlled by the rule-based paradigm, using adaptation procedures and heuristics in the form of implication. Sensibly chosen meta-rules can substantially improve the effectiveness of the system.

The problem of adaptation is quite serious when a cluster of similar cases is replaced by one representative only - to avoid a high level of redundancy of the case library. The level of similarity can be low for marginal cases of the cluster. So, adaptation is more important here.
Three main categories of rules can be found in the rule-based module:

- Several general heuristics can contribute to the optimal solution search of a very wide class of tasks.
- However, the dominant part of the knowledge support is based on a domain-specific rule.
- For a higher efficiency, metarules are also attached to the module. This "knowledge about knowledge" can considerably contribute to a smooth reasoning process.

While involvement of an expert is relatively low for case-based reasoning module, the rules are mainly based on expert's knowledge. However, some pieces of knowledge can also be obtained by data mining.

7.3 Similarity measurement of state-based specifications

Retrieval schemes proposed in the literature can be classed based upon the technique used to index cases during the search process (Atkinson, 1998): (a) classification-based schemes, which include keyword or feature-based controlled vocabularies; (b) structural schemes, which include signature or structural characteristics matching; and (c) behavioral schemes; which seek relevant cases by comparing input and output spaces of components.
The problem to be solved arises how to measure the similarity of state-based specifications for retrieval. Incidentally, similarity measurements for relational specifications have been resolved by Jilani, et al. (2001). The primary approach to the current application includes some equivalents of abstract data type signatures, belonging to structural schemes, and keywords, belonging to classification schemes. While the first alternative means for this purpose to quantify the similarity by the topological characteristics of associated finite automata state-transition graphs, such as number and placement of loops, the second one is based on a properly selected set of keywords with subsets identifying individual patterns. The current research task of our group focuses on experiments enabling to compare those alternatives.

8. Conclusions

The book chapter stems from the paper (Sveda, Vrba and Rysavy, 2007) and complements it by TLA specifications. The original contribution consists in proposal how to represent a system's formal specification as an application pattern structure of specification fragments. Next contribution deals with the approach how to measure similarity of formal specifications for retrieval in frame of case-based reasoning support. The above-presented case studies, which demonstrate the possibility to effectively reuse concrete application pattern structures, have been excerpted from two realized design cases.
The application patterns, originally introduced as "configurations" in the design project of petrol pumping station control technology based on multiple microcontrollers (Sveda, 1996), were effectively -- but without any dedicated development support -- reused for the project of lift control technology (Sveda, 1997). The notion of application pattern appeared for the first time in (Sveda, 2000) and was developed in (Sveda, 2006). By the way, the first experience of the authors with case-based reasoning support to knowledge preserving

development of an industrial application was published in (Sveda, Babka and Freeburn, 1997).

8. Acknowledgements

The research has been supported by the Czech Ministry of Education in the frame of Research Intentions MSM 0021630528: Security-Oriented Research in Information Technology and MSM 0021630503 MIKROSYN: New Trends in Microelectronic Systems and Nanotechnologies, and by the Grant Agency of the Czech Republic through the grants GACR 102/08/1429: Safety and Security of Networked Embedded System Applications and GACR 201/07/P544: Framework for the deductive analysis of embedded software.

10. References

Alexander, C. (1977) A Pattern Language: Towns / Buildings / Construction, Oxford University Press.

Alur, R. and T.A. Henzinger (1992) Logics and Models of Real Time: A Survey. In: (de Bakker, J.W., et al.) Real-Time: Theory in Practice. Springer-Verlag, LNCS 600, 74-106.

Arora, A. and S.S. Kulkarni (1998) Component Based Design of Multitolerant Systems. IEEE Transactions on Software Engineering, 24(1), 63-78.

Atkinson, S. (1998) Modeling Formal Integrated Component Retrieval. Proceedings of the Fifth International Conference on Software Reuse, IEEE Computer Society, Los Alamitos, California, 337-346.

Coad, P. and E.E. Yourdon (1990) Object-Oriented Analysis, Yourdon Press, New York.

Frakes, W.B. and K. Kang (2005) Software Reuse Research: Status and Future. IEEE Transactions on Software Engineering, 31(7), 529-536.

Gamma, E., R. Helm, R. Johnson and J. Vlissides (1995) Design Patterns -- Elements of Reusable Object-Oriented Software, Addison-Wesley.

Geppert, B. and F. Roessler (2001) The SDL Pattern Approach – A Reuse-driven SDL Design Methodology. Computer Networks, 35(6), Elsevier, 627-645.

Henninger, S. (1997) An Evolutionary Approach to Constructing Effective Software Reuse Repositories. Transactions on Software Engineering and Methodology, 6(2), 111-140.

Henninger, S. (1998) An Environment for Reusing Software Processes. Proceedings of the Fifth International Conference on Software Reuse, IEEE Computer Society, Los Alamitos, California, 103-112.

Holtzblatt, L.J., R.L. Piazza, H.B. Reubenstein, S.N. Roberts and D.R. Harris (1997) Design Recovery for Distributed Systems. IEEE Transactions on Software Engineering, 23(7), 461-472.

Jacobson, L. (1992) Object-Oriented Software Engineering: A User Case-Driven Approach, ACM Press.

Jilani, L.L., J. Deshamais and A. Mili (2001) Defining and Applying Measures of Distance Between Specifications. IEEE Transactions on Software Engineering, 27(8), 673-703.

Johnson, R.E. (1997) Frameworks = (Components + Patterns), Communications of the ACM, 40(10), 39 42.

Kolodner, J. (1993) Case-based Reasoning, Morgan Kaufmann, San Mateo, CA, USA.
Lamport, L. (1994) Temporal Logic of Actions. ACM Transactions on Programming Languages and Systems, 16(3) :872-923.
Lamport, L. (2002) Specifying Systems. Addison-Wesley, 2002.
Mili, R., A. Mili, and R.T. Mittermeir (1997) Storing and Retrieving Software Components: A Refinement Based System. IEEE Transactions on Software Engineering, 23(7), 445-460.
Sen, A. (1997) The Role of Opportunity in the Software Reuse Process. IEEE Transactions on Software Engineering, 23(7), 418-436.
Shaw, M. and D. Garlan (1996) Software Architecture, Prentice Hall.
Soundarajan, N. and S. Fridella (1998) Inheritance: From Code Reuse to Reasoning Reuse. Proceedings of the Fifth International Conference on Software Reuse, IEEE Computer Society, Los Alamitos, California, 206-215.
Sutcliffe, A. and N. Maiden (1998) The Domain Theory for Requirements Engineering. IEEE Transactions on Software Engineering, 24(3), 174-196.
Sveda, M. (1996) Embedded System Design: A Case Study. IEEE Proc. of International Conference and Workshop ECBS'96, IEEE Computer Society, Los Alamitos, California, 260-267.
Sveda, M., O. Babka and J. Freeburn (1997) Knowledge Preserving Development: A Case Study. IEEE Proc. of International Conference and Workshop ECBS'97, Monterey, California, IEEE Computer Society, Los Alamitos, California, 347-352.
Sveda, M. (1997) An Approach to Safety-Critical Systems Design. In: (Pichler, F., Moreno-Diaz, R.) Computer Aided Systems Theory, Springer-Verlag, LNCS 1333, 34-49.
Sveda, M. (2000) Patterns for Embedded Systems Design. In: (Pichler, F., Moreno-Diaz, R., Kopacek, P.) Computer Aided Systems Theory--EUROCAST'99, Springer-Verlag, LNCS 1798, 80-89.
Sveda, M. and R. Vrba (2006) Fault Maintenance in Embedded Systems Applications. Proceedings of the Engineering of Computer-Based Systems. Proceedings of the Third International Conference on Informatics in Control, Automation and Robotics (ICINCO 2006), INSTICC, Setúbal, Portugal, 183-186.
Sveda, M., R. Vrba and O. Rysavy (2007) Pattern-Driven Reuse of Embedded Control Design -- Behavioral and Architectural Specifications in Embedded Control System Designs. Proceedings of Fourth International Conference on Informatics in Control, Automation and Robotics (ICINCO 2007), INSTICC, Angers, FR, pp. 244-248.
Turner, K.J. (1997) Relating Architecture and Specification. Computer Networks and ISDN Systems, 29(4), 437-456.
van Lamsweerde, A. and L. Willemet (1998) Inferring Declarative Requirements Specifications from Operational Scenarios. IEEE Transactions on Software Engineering, 24(12), 1089-1114.
Xinyao, Y., W. Ji, Z. Chaochen and P.K. Pandya (1994) Formal Design of Hybrid Systems. In: (Langmaack, H., W.P. de Roever and J. Vytopil) Formal Techniques in Real-Time and Fault-Tolerant Systems, Springer-Verlag, LNCS 863, 738-755.
Zaremski, A.M. and J.M. Wing (1997) Specification Matching of Software Components. ACM Trans. on Software Engineering and Methodology, 6(4), 333-369.

Frontiers in Robotics, Automation and Control

Edited by Alexander Zemliak

ISBN 978-953-7619-17-6
Hard cover, 450 pages
Publisher InTech
Published online 01, October, 2008
Published in print edition October, 2008

This book includes 23 chapters introducing basic research, advanced developments and applications. The book covers topics such us modeling and practical realization of robotic control for different applications, researching of the problems of stability and robustness, automation in algorithm and program developments with application in speech signal processing and linguistic research, system's applied control, computations, and control theory application in mechanics and electronics.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Miroslav Švéda, Ondřej Ryšavý and Radimir Vrba (2008). Pattern-driven Reuse of Behavioral Specifications in Embedded Control System Design, Frontiers in Robotics, Automation and Control, Alexander Zemliak (Ed.), ISBN: 978-953-7619-17-6, InTech, Available from: http://www.intechopen.com/books/frontiers_in_robotics_automation_and_control/pattern-driven_reuse_of_behavioral_specifications_in_embedded_control_system_design

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821