Supporting Automated Verification of Reconfigurable Systems with Product Lines and Model Checking

Faiz Ul Muram\textsuperscript{1}, Samina Kanwal\textsuperscript{2} and Muhammad Atif Javed\textsuperscript{3}

\textsuperscript{1}School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
\textsuperscript{2}National University of Sciences and Technology, Islamabad, Pakistan
\textsuperscript{3}RISE Research Institutes of Sweden, Västerås, Sweden

Keywords: Reconfigurable Systems, Product Lines, Model Transformations, Model Checking, Formal Methods and LTL.

Abstract: The capability to dynamically reconfigure in response to change of mode or function, failures, or unanticipated hazardous conditions is fundamental for many critical systems. The modelling and verification of such systems are frequently carried out with product lines and model checking, respectively. At first, the objectives and related requirements of reconfigurable systems are mapped to a feature model, whereas the units related to operational modes are selected in individual configurations. After that, the proposed approach performs automated transformation of particular models into formal constraints and descriptions for leveraging the analytical powers of model checking techniques; the formal verification of completeness, consistency and conflict is carried out with NuSMV model checker. Finally, in circumstances when the counterexample is produced, its analysis is performed for the identification of corresponding problems and their resolutions. The applicability of the proposed approach is demonstrated through case study of attitude and orbit control system.

1 INTRODUCTION

The principal intention of reconfigurable systems is to enhance the responsiveness in consequence to mode or function changes, environmental conditions and unexpected failures (Muram et al., 2020). The reconfigurable systems possess the advantages of both dedicated product lines and of flexible systems. In particular, they focus on customized flexibility that can be supported through product lines. The product lines have been used for the identification and systematization of commonalities and variabilities to concurrently engineer a set of scenarios; the achievement of a single configuration is based on the selection and composition of commonalities and variabilities (Javed and Gallina, 2018; Javed et al., 2019). The integration between product line and model checking is essential for the formal verification of reconfigurable system behaviour against its formal requirements that are often expressed in temporal logic (Gan et al., 2014).

There exist several efforts to apply the model checking technique for product line verification, for example, (Gruler et al., 2008; Lauenroth et al., 2009; Lochau et al., 2016). However, previous approaches have not considered the automated transformations of product lines. These approaches often assume that formal descriptions and constraints of the product line can be easily created. Unfortunately, this makes the approaches hard to apply in practice because creating formal descriptions and constraints requires the underlying knowledge of formal techniques (Muram et al., 2016; Muram et al., 2017; Muram et al., 2019). Moreover, this task is often accomplished in a laborious and manual manner, which is also error-prone (Gruler et al., 2008; Lauenroth et al., 2009). In case of violations the results produced by model checkers (e.g., counterexamples) are rather cryptic and verbose (Muram et al., 2015; Muram et al., 2019). As a consequence, they are difficult to interpret and understand for those who have limited knowledge of the underlying formal techniques.

This paper focuses on the automated transformations and formal verification of reconfigurable systems. In particular, the objectives and related requirements of reconfigurable systems are mapped to a feature model, which in turns automatically transformed into the formal constraints i.e., Linear Temporal Logic (LTL) (Pnueli, 1977); whereas the units related to operational modes selected in individual configurations are transformed into state based Symbolic Model Verifier (SMV) (Cimatti et al., 1999) language. These transformations are achieved by us-
ing Eclipse Xtend. Specifically, the mapping rules are defined to transform the feature model and configurations into formal constraints and descriptions. This way, our approach helps to alleviate the burden of manually encoding formal constraints and descriptions, and therefore, increase productivity and avoid potential translation errors. The formal verification of completeness, consistency and conflict is carried out with the NuSMV\textsuperscript{1} 2.6.0, a new version of symbolic model checker. Completeness considers whether a set of configurations satisfy the system objectives and related requirements. Consistency checking examines the correctness of configurations against the structure and sequence of the system. Conflict verifies whether the configurations are compatible with the system constraints or not. In circumstances when the counterexample is produced by the model checker, its analysis is performed for the identification of corresponding problems and their resolutions. The applicability and technical feasibility of the proposed approach is demonstrated through case study of Attitude and Orbit Control System (AOCS).

The rest of this paper is organized as follows: Section 2 describes the tool-supported method for the formal verification of reconfigurable systems. Section 3 demonstrates the effectiveness of proposed approach through AOCS product line scenario. Section 4 discusses related work. Section 5 concludes the paper and presents future research directions.

2 APPROACH

The modern variable systems are often composed of several distinct sensors, controllers and actuators that can operate in both isolation and conjunction. For such systems, the capability to adjust, in particular, the reconfiguration in consequences to mode or function changes, environmental conditions and system failures is perceived as fundamental. Product lines provide the means to handle (re)configurations of systems. To be able to build a product line, the objectives and related requirements are mapped to a feature model; however, for (re)configurations, the scenario information or operational modes could be used (Muram et al., 2020). The principal focus of our approach is to formally verify the completeness, consistency and conflict in reconfigurable systems. The violations can be produced when the configurations are incomplete with respect to the system objective and related requirements, inconsistent with the organization and sequence of the system (i.e., decomposition hierarchy and groups), and incompatible with the system (cross-tree) constraints. Counterexample analysis detects the violation cause(s) and provide measures to make the configurations valid. An overview of our approach is shown in Figure 1. In the following sections, we describe each step of our approach.

1\textsuperscript{1}http://nusmv.fbk.eu/

Figure 1: An Overview of the Proposed Approach

2.1 Generating LTL Constraints

In this subsection, we present our algorithmic solution for the generation of formal constraints from a feature model. The relationships between features (e.g., decomposition hierarchy, groups and cross-tree constraints) need to be represented in an appropriate formalism so that the selection or deselection of features will become the formal constraints for the configuration(s). In this context, LTL is used for describing the temporal relationships or properties among the features (Pnueli, 1977). LTL extends the classical propositional logic, for instance, negation (¬φ), implication (→), conjunction (∧), and disjunction (∨) with several future operators, such as Fφ (“Finally/Sometime”), Gφ (“Globally/Always”) and φ₁ U φ₂ (“Until”). To make the formulation of some formulas significantly more concise and intuitive, we have also used the LTL past operators, to reason about previous states and transitions, such as Hφ (“Historically”) and Oφ (“Once”).

The construction of LTL formulas (constraints) for formal verification of reconfigurable systems is a highly knowledge intensive endeavour. Therefore, the mapping rules are defined to formally represent the semantics of a feature model elements. By using these mapping rules, an input feature model is automatically transformed to the corresponding LTL formulas. Table 1 summarises the modelling elements of a feature model along with their definitions and mapping rules that constitutes the relationships between features, such as optional and manda-
<table>
<thead>
<tr>
<th>Graphical Symbols</th>
<th>Relationships Definition</th>
<th>Mapping Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Mandatory: If parent feature F1 is selected in a product, then child feature F2 must be selected. This indicates the commonality.</td>
<td>( G (F1 \rightarrow F \land F2) \land H (F2 \rightarrow O \land F1) )</td>
</tr>
<tr>
<td>F2</td>
<td>Optional: If parent feature F1 is selected in a product, then child feature F2 may be selected or not. This expresses the variability. In particular, F2 will be selected if F1 and isSelected condition are true.</td>
<td>( G ((F1 \land \text{isSelected} \rightarrow F \land F2) \lor (F1 \rightarrow F \lor F2)) )</td>
</tr>
<tr>
<td>P</td>
<td>Alternative (Xor): The semantic represents the case in which only one feature of the children needs to be selected when its parent feature P is part of the product.</td>
<td>( (P \rightarrow F ((F1 \land \neg \ldots \land \neg Fn) \lor (\neg F1 \land \neg \ldots \land \neg Fn)) )</td>
</tr>
<tr>
<td>F1,...,Fn</td>
<td>Or: If parent feature P is selected in a product, then at least one of the children must be selected. The traversal of features depend on the evaluation of isSelected conditions.</td>
<td>( G ((P \land \text{isSelected}_1) \rightarrow F \land F1) \lor \ldots \lor G ((P \land \text{isSelected}_n) \rightarrow F \land Fn) )</td>
</tr>
<tr>
<td>F1 ← F2</td>
<td>Excludes: Both features cannot be part of the same product. If F1 is selected then F2 cannot not selected, and vice versa.</td>
<td>! (F1 \land \neg F2), or more complex,</td>
</tr>
<tr>
<td></td>
<td>(i)F (F1) \rightarrow (! F1 \lor \text{isSelected})</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(ii)F (F2) \rightarrow (! F2 \land \text{isSelected})</td>
<td></td>
</tr>
</tbody>
</table>

The generate_ltl_formulas function is not realised as a single function but rather a polymorphism of multiple functions. That is, depending on the type of relationships between features i.e., decomposition hierarchy and cross-tree constraints, a particular function for generating LTL formulas for that relationship will be invoked. The functions can have the same name but require different input types. This can be obtained in traditional programming languages by using the “if/then/else” or “switch/case” construct. The generation of Mandatory feature is presented in Algorithm 1 (Line 21–25). For code generation the string templates are surrounded by the pair of a triple single quotes (```). However, the terminals for interpolated expression, called guillemets (« and ») are used to represent the parametrised placeholders that will be bound to and substituted with the actual values extracted from the input model elements by the Xtend engine. In NuSMV, LTL formulas are introduced by the LTLSPEC keyword.

### 2.2 Generating SMV Descriptions

This subsection presents the automated transformation of a set of configurations into formal SMV model
The basic purpose of the SMV language is to describe the transition relation of a finite Kripke structure. The encoding of configurations in terms of SMV descriptions provides the infrastructure to facilitate the verification of completeness, consistency, and conflicts with a feature model, and especially, analysing the verification results to provide useful feedback for aiding the manager/developers in resolving violations. Similar to the generation of LTL formulas, the mapping of configurations into SMV descriptions is obtained by using Xtend framework. As described in Section 2.1, three helper functions are created. First two functions are same, however, the \texttt{generate_smv_model}(f) function is responsible for generating SMV descriptions for a set of configurations. We illustrate the skeleton of the function \texttt{generate_smv_model}(f) in Algorithm 2.

The SMV model consists of several modules, which are used to encapsulate variables deceleration and assignments. The identifier after the keyword \texttt{MODULE} is the name associated with the module. An instance of a module is created using the \texttt{VAR} declaration. In particular, the features are specified by boolean state variables in the section \texttt{VAR} and their corresponding transition relations are described in the section \texttt{ASSIGN} by a combination of two functions given in NuSMV (Cimatti et al., 1999). These variables are initialised with initial values as shown in the \texttt{init(identifier)} clause, whereas the function \texttt{next(identifier)} defines the next state of the variable based on current states. It is often combined with the branching structure “\texttt{case/esac}” for selecting one of many possible choices. The state is initially set to False. However, if the branch condition(s) are satisfied, it is changed to a True state. The branch condition(s) can be a guard expression and/or finishing of the preceding state. The feature’s state shall be switched back to False after finishing the execution. Similar to \texttt{generate_ltl_formulas}(f), the function \texttt{generate_smv_model}(f) is not realised as a single function but rather a polymorphism of multiple functions.

A consistent and complete set of configurations is obtained by selecting a complete group of features in a manner that follows a correct feature hierarchy. Moreover, the semantics of the configurations should not be contradicted with constraints (requires, excludes) of the system (i.e., feature model). It is assumed that two features cannot have the same name. This assumption is rather realistic because the same name can imply ambiguity problems during (re)configuration of systems. While selecting the configurations, if a parent feature is selected (or deselected) then all mandatory child-features linked with a particular parent feature will be selected (or deselected). The \texttt{ASSIGN} section defines the transition relation of features. The child-feature is initially set to false. However, if the condition(s) are satisfied, it is changed to a true state (see Line 15), as shown in Figure 2. The feature’s state shall be switched back to false after the execution.
The Xor-groups (Alternatives) are transformed as a set of configurations which show that exactly one child-feature will be selected in each configuration. In reality, the developers/corresponding manager(s) are responsible for the exclusiveness of conditions, i.e., selection of the child-feature based on a specific configuration. Figure 3 shows the rules for mapping an Alternative relationship into SMV descriptions. For the purpose of verification, it is possible to initialise a constraint, namely isSelected with the boolean values that is evaluated to true. However, in cases when the different types of variables may have dependencies among constraints, temporary variables of enumerated types can be introduced to handle them. Accordingly, a temporary variable named tem_alternative_k is defined, where k is an incrementally generated number. This variable is used as a program counter to determine which procedure, function or feature state is being executed at present. The variable tem_alternative_k has an enumerated type that includes a normal state “undetermined” and the values corresponding to the configurations or child-features (Line 7). It might be noted that the non-deterministic assignment is a powerful means provided by the NuSMV model checker for exhaustively exploring multiple possible execution paths yielded by the values of an enumerated state. The evaluation of the conditions is made using a “case/esac” construct (Line 16–19). The next state of tem_alternative_k will be either selected_1, selected_2 or selected_3 (Line 22, 27).

An Or relationship represents that any number of features can be selected in a configuration instead of one and only one. We initialised a constraint, namely isSelected with the boolean values that is evaluated to true when the corresponding element is selected. We use the logical AND operator (“&”) to represent all incoming conditions, as shown in Figure 4. The cardinality <min..max> might be applied, where min denotes a lower bound limit and max denotes upper bound limit within a group of features the number of features that can be part of a configuration.

### 2.3 Formal Verification and Dealing with Violations

This subsection discusses the identification and resolution of violations (i.e., incompleteness, inconsistencies and conflicts) in the reconfigurable systems. The formal verification is achieved by using the NuSMV model checker that takes the generated SMV model (descriptions) and LTL formulas, and exhaustively explore the deviations of an LTL formula by traversing complete state space. In case an LTL formula does not satisfy the SMV model, NuSMV will generate a

```plaintext
1 MODULE main
2 VAR
3 «ParentFeature» : boolean;
4 «ChildFeature1» : boolean;
5 ...– temporary variable
6 «ChildFeature3» : boolean;
7 ASSIGN
8 init({«ParentFeature»}) := TRUE;
9 next({«ParentFeature»}) := case
10 «ParentFeature» : TRUE;
11 «ChildFeature» : FALSE;
12 TRUE : «ParentFeature»;
13 esac;
14 init({«ChildFeature»}) := FALSE;
15 next({«ChildFeature»}) := case
16 «ParentFeature» : TRUE;
17 «ChildFeature» : FALSE;
18 TRUE : «ChildFeature»;
19 esac;
20 ...
21 -- if the parent feature is not a root
22 init({«tem_alternative_k»}) := undetermined;
23 next({«tem_alternative_k»}) := case
24 «ParentFeature» & ({
25 «tem_alternative_k» = undetermined} : «selected_1
26 »,..., «selected_3»);
27 TRUE : undetermined;
28 esac;
29 init({«ChildFeature1»}) := FALSE;
30 next({«ChildFeature1»}) := case
31 «tem_alternative_k» = «selected_1
32 » : TRUE;
33 «ChildFeature1» : FALSE;
34 esac;
35 init({«ChildFeature3»}) := FALSE;
36 next({«ChildFeature3»}) := case
37 «tem_alternative_k» = «selected_3
38 » : TRUE;
39 «ChildFeature3» : FALSE;
40 esac;
```

Figure 2: Generic rules for SMV description

Figure 3: Mapping rules for Alternatives
column_counterexample that consists of the execution traces of the SMV descriptions leading to the deviation. The incompleteness may occur due to the absence of units or features in configurations with respect to system objectives and requirements. The inconsistency of configurations may happen when a hierarchical or sequential order is not followed, such as inaccurate relation or groups between features/units, or misplacement of features. Conflict occurs when a cross-tree constraint is violated, for instance, an optional feature is excluded, however, due to the requires constraint, it has to be included in some configurations. The analysis of counterexample not only detects the typical possible causes of incompleteness, inconsistency, and conflict but also provides the recommendations to resolve the specific deviation.

To locate the causes of deviations, the verification result (i.e., output trace file) is scrutinised and parsed to identify the false LTL formulas. The extracted formulas and SMV descriptions together with mapping rules for a feature model are traversed to find out why the particular configuration(s) deviate from the specification defined in a feature model. This is performed in three steps. First, the absence of units or missing obligatory feature cause (either one or multiple features/units could be missing) is detected and the corrective measures, i.e., add the missing obligatory features/units is suggested. Second, the hierarchical dependency and sequence between features are scrutinised from the SMV descriptions, for example, multiplicity causing the deviations of the LTL formulas are located and appropriate recommendations, i.e., remove or replace the features or units are presented. Finally, the constraints between features are scrutinised, for instance, requires or excludes causing the deviation of the LTL formulas are located and appropriate recommendations, i.e., insert or delete features are provided. Based on the deviation causes and given recommendations, the systems can be reconfigured and transformed again into their formal descriptions, and then will be re-verified until no more deviations are detected.

3 CASE STUDY

In this section, we briefly describe a variable system that belongs to a space domain, in particular, the AOCS (Javed et al., 2019). It consists of sensors, actuators, software, and ground support equipment to control the satellite’s attitude and orbit. In the ECSS-E-ST-60-30C standard, the AOCS requirements, operational objectives, tailoring rules and customer specifications are presented. The standard objectives and requirements for AOCS are mapped into a feature model, whereas tailoring rules, customer specifications, units related to AOCS operational modes are selected in individual configurations (Javed et al., 2019). In this paper, we focus on four different configurations of AOCS, which are: (i) Sun Sensors to Thrusters (SSTH); (ii) Sun Sensors to Reaction Wheels (SSRW); (iii) Star Tracker to Thrusters (STTH); and (iv) Star Tracker to Reaction Wheels (STRW). Figure 5 shows the feature model of AOCS that presents the different allowed combinations of sensors, actuators, as well as the associated functional software modules.

- **Sensing Principles**: In SSTH and SSRW configurations, Sun Sensors are used as the primary sensor in combination with a Magnetometer to provide full attitude determination capability. In STTH and STRW configurations, a Star Tracker is used as a primary attitude sensor. In all configurations, the attitude is estimated using a kinematic (Kalman) filter-based estimation for which Gyro measurements are an exogenous input.

- **Actuation Principles**: In SSTH and STTH configurations, the spacecraft attitude is modified using a Thruster actuator, whereas in SSRW and STRW configurations, the spacecraft attitude is primarily controlled using Reaction Wheels.

- **Software Functional Modules**: They are classified into different functional groups, such as
Sensor Processing, Guidance, Estimation, Control and Command Distribution.

- **Operational Modes**: The AOCS consists of several modes, for instance, in case of major anomaly a Safe Mode is automatically initiated to reach and control safe pointing attitude and angular rates. A Normal Mode concerns the mission level performances of spacecraft during the operational phase. Typically, SSTH variant would be used for a Safe Mode. It might be used in combination with SSRW for long term safety and variant STRW for a Normal Mode.

To demonstrate the qualification of AOCS configurations, the formal verification is performed by using the NuSMV model checker. In particular, the AOCS feature model and configurations are automatically transformed into LTL formulas and SMV descriptions by applying mapping rules described in Section 2.1 and Section 2.2, respectively. The generated SMV descriptions and LTL formulas are combined into one input file and executed by the NuSMV model checker version 2.6.0. The evaluation is conducted on a regular computer equipped with a 2.90 GHz i7 processor and sixteen gigabytes of memory running Windows 10. The approach is implemented using Java and automated transformations have been realised using Eclipse Xtend. Figure 6 shows the verification results including the list of satisfied and unsatisfied LTL formulas. The NuSMV model checker generator performs a counterexample analysis to provide insights into the system behavior.

---

2 See http://www.eclipse.org/xtend

Figure 6: NuSMV Verification Results
erates a counterexample demonstrating a sequence of permissible state executions leading to a state in which the deviation occurs in LTL formula. By looking at the results, we found that four LTL formulas are false. In order to identify the deviations causes, the counterexample analysis is performed (as depicted in Section 2.3). In this case, the specification of AOCS system is deviated due to (i) incomplete configurations, i.e., missing GroundCommand feature, which is required by AttitudeGuidance; (ii) inconsistency in hierarchical dependency and sequence: (a) Gyro feature can only be selected after its parent feature Sensors is selected, and (b) when parent feature AttitudeandOrbitControlSystem is selected, then mandatory child feature Sensors must be selected, subsequently Gyro would be selected; and (iii) conflict: an optional feature StarTracker is added, but due to the excludes constraint, it has to be excluded in SSRW configuration. These deviations can be resolved by adding GroundCommand feature, removing StarTracker feature in the SSRW configuration and correcting the sequence of AttitudeandOrbitControlSystem, Sensors and Gyro, respectively. NuSMV took three seconds to verify AOCS system, which is quite reasonable. Without the counterexample analysis, users would have to study and investigate the syntax and semantics of the trace file in order to determine the relationship between the execution traces and models, and then locate the corresponding violations manually.

4 RELATED WORK

The work presented in (Gruler et al., 2008) extended the process algebra Calculus of Communicating Systems (CCS) by introducing a variant operator that allows to model an alternative choice between two processes. A multivalued modal $\mu$-calculus is used for specifying the properties of individual configurations of a PL-CCS program. However, the verification using a model checker is not performed that is prerequisite for practical evaluation. For incremental verification of software product lines, a delta-oriented extension of CSS (DeltaCCS) is described in (Lochau et al., 2016). A core product (process) is first verified against a given property by using Maude model checker, then different variants are derived from the core process by applying CCS Delta sets. Lauenroth et al. (Lauenroth et al., 2009) presented a model-checking approach to verify every permissible product specified with I/O-automata against provided Computational Tree Logic (CTL) properties. The authors just used three operators (EX, EU and EG) to define one property of each type. Classen et al. (Classen et al., 2011) focused on the feature-oriented extension of SMV language called f/SMV that is equivalent to high-level representation of finite transition systems. An algorithm on top of the symbolic model-checking is presented to check whether a set of valid products in the feature diagram (f/SMV) satisfies one or more feature CTL properties. Shi et al. (Shi et al., 2014) presented the Bilattice-based Feature Transition Systems (BFTSs) for modelling partial (i.e., incomplete) software product line designs, while the Action CTL formulas are used to express system behavioural properties. To carry out the model checking with exiting $\chi$Chek engine, the translations from BFTS to multi-valued Kripke structure and from ACTL to CTL formulas are presented. Beek et al. (ter Beek et al., 2016) presented QPFlan specifications to model the quantitative properties such as price and weight of a product line, and a prototypical Maude interpreter integrated with Z3 and MultiVeStA model checker. Previous studies on the model checking of product lines have not considered the automated transformations of feature model and configurations into LTL constraints and formal descriptions. In addition, the counterexample analysis for identifying the causes of deviations and their resolutions has not been considered.

Gan et al. (Gan et al., 2014) used the NuSMV model checker to verify the design of an AOCS. They manually translated the AOCS implementation i.e., Ada source code abstractions to SMV language. The required system behaviour that is extended state machine diagrams with prioritized transitions are translated into LTL properties. However, they have not considered the product lines. The automatic transformations of sequence diagrams (Muram et al., 2016), activity diagrams (Muram et al., 2019) and service choreographies (Muram et al., 2015; Muram et al., 2017) are investigated for the containment checking problem. In this paper, we performed the automated transformations and formal verification of reconfigurable systems modelled in a product line.

5 CONCLUSIONS

This paper targets the integration of product line and model checking for the formal verification of reconfigurable system behaviour against its formal requirements. To achieve this, the objectives and related requirements of reconfigurable system are mapped to a feature model, whereas the units related to operational modes are selected in individual configurations. To leverage the NuSMV model checker for
the formal verification, the automated transformations of these models into LTL constraints and formal descriptions are performed. Subsequently, the analysis of model checker results is performed for the identification and resolution of deviations (i.e., incompleteness, inconsistency and conflict), in order to satisfy the configuration(s) with a feature model. The applicability of the proposed approach is demonstrated through AOCS family/product line. It is noteworthy that the proposed approach is generally applicable to the broad range of scenarios and domains.

In the future, we plan to perform automatic extraction of feature and configuration models from document files. We also plan to consider additional scenarios and application, such as electric quarry site (Javed et al., 2020). Another direction for future work is to attach the evidence obtained from runtime model checking with the assurance cases that are constructed to provide comprehensive, logical and defensible justification of the safety and security of a reconfigurable production system (Muram et al., 2020).

ACKNOWLEDGEMENTS

This work is partially supported by FiC (Future factories in the Cloud) project funded by SSF (Swedish Foundation for Strategic Research). The third author has also participated during the tenure of an ERCIM “Alain Bensoussan” Fellowship Programme.

REFERENCES


