Towards Variant Management and Change Impact Analysis in Safety-oriented Process-Product Lines

Muhammad Atif Javed and Barbara Gallina
Mälardalen University, Västerås, Sweden
{muhammad.atif.javed,barbara.gallina}@mdh.se

Anna Carlsson
OHB, Stockholm, Sweden
anna.carlsson@ohb-sweden.se

ABSTRACT

In safety-critical (software) systems, safety management embraces both processes and products, which due to e.g., product's upgrade, tend to be tailored, giving rise to safety-oriented product lines and corresponding safety-oriented process lines. To tailor these lines systematically, their inter-dependencies would have been taken into consideration. To date, however, no satisfying implemented solution is available on the shelf. Accordingly, this paper focuses on the co-engineering of process and product lines. At first, the process and product lines need to be established for which the integration between Eclipse Process Framework (EPF) Composer, Composition with Guarantees for High-integrity Embedded Software Components Assembly (CHESS) Tool and Base Variability Resolution (BVR) Tool is achieved; they are process engineering, product design and variant management solutions, respectively. After that, the process and product lines are integrated. This is done for cross-dimension variant management and change impact analysis. The applicability of the integrated lines is illustrated for the attitude and orbit control subsystem.

CCS CONCEPTS

• **Software and its engineering → Software system models**; **Reusability**; **Software product lines**;

KEYWORDS

Process Engineering, EPF Composer, Product Design, CHESS Tool, Process-Product Lines, BVR Tool and Change Impact Analysis.

ACM Reference Format:
Muhammad Atif Javed and Barbara Gallina and Anna Carlsson. 2019. Towards Variant Management and Change Impact Analysis in Safety-oriented Process-Product Lines. In *The 34th ACM/SIGAPP Symposium on Applied Computing (SAC '19), April 8–12, 2019, Limassol, Cyprus.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3297280.3297634

1 INTRODUCTION

The safety-oriented processes and products tend to be reused, modified and extended [7][9]. This is dependent on the specific aspects of each project, such as criticality classification, performance and functional specifications, hardware characteristics, and environmental conditions. Besides that, the design and implementation languages are chosen for the projects. To engineer the process and product lines, either the support for variability modelling and management might be incorporated and implemented in the process engineering and product design solutions [4], or otherwise the integration with variability management solution needs to be achieved [6].

In this paper, we develop a solution for variant management and change impact analysis in process and product lines. This solution is built on top of the integration [6] between Eclipse Process Framework (EPF) Composer[1] (recently migrated to Eclipse Neon 4.6.3 [5]) utilized for process engineering and Base Variability Resolution (BVR) Tool[2] utilized for orthogonal variant management [10]. The integration is extended to product design [8] for which Composition with Guarantees for High-integrity Embedded Software Components Assembly (CHESS) Toolset[3] is integrated. This solution enables the specification of cross-cutting constraints between the variability models, joining of resolutions and simultaneous execution of realization fragments belonging to multiple base models. The applicability of the integrated lines is illustrated for the development of attitude and orbit control subsystem.

The rest of this paper is organized as follows: Section 2 presents the related work. Section 3 discusses the establishment and integration of process and product lines. Section 4 demonstrates usability of the proposed integration. Section 5 concludes the paper and sketches future research directions.

2 RELATED WORK

The processes and products have to be tailored by taking their inter-dependencies into consideration. Prause et al. [9] described the tailoring of process requirements for space product assurance; the applicable requirements in European Cooperation for Space Standardization (ECSS) standards are integrated. Their objective is to assure the quality of products developed for individual customers for which the critical functions in a space flight mission are taken into consideration. Gallina [4] discusses the need for variant management and impact analysis in integrated process, product and assurance case lines. Andrzej Kobylinski [7] focused on the relationships between software quality characteristics (ISO/IEC 25010) and software life cycle processes (ISO/IEC 12207). In particular, the relationships between process and product artefacts are mentioned in a table. To date, however, the published studies have not integrated the process-product lines.

3 METHODOLOGY

To engineer the process and product lines, the EPF Composer, CHESS Toolset and BVR Tool are integrated. The BVR Tool supports

SAC '19, April 8–12, 2019, Limassol, Cyprus

ACM ISBN 978-1-4503-5933-7/19/04.
https://doi.org/10.1145/3297280.3297634

[1] https://www.eclipse.org/epf/
[2] https://github.com/SINTEF-9012/bvr
[3] https://www.polarsys.org/chess/

orthogonal variant management for which communication with other tools is needed for mapping the elements of target configurations and variability abstractions in BVR Tool. The generation of target configurations is performed with VSpec, Resolution and Realization editors. Besides the individual process and product lines, their integration is supported. An overview of the integrated process-product lines is illustrated in Figure 1.

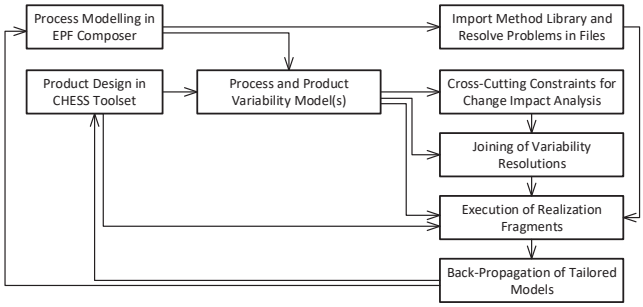

Figure 1: Establishment of Process-Product Lines

3.1 Integrating the EPF Composer, CHESS Toolset and BVR Tool

For the establishment of process and product lines, variability realization of XMI files (Section 3.1.1), back-propagation into CHESS project and EPF library, and the visualization of generated models in CHESS editor (Section 3.1.2) are supported.

3.1.1 Variability Realization. The integration between EPF Composer and BVR Tool is implemented as Eclipse plugin. The interested reader may refer to [6] for an explanation of the problems, which were resolved for supporting the placement and replacement fragments within the realization editor of BVR Tool.

The CHESS Toolset is built on top of Eclipse Papyrus. Similar to the Papyrus, the CHESS model is stored in .di, .notation and .uml files. In order to visualize the diagrams, the .di file is opened with the Papyrus editor, in which the dragged model variants from model explorer or palette are dropped. As a consequence, the style information is recorded in the .notation file. The model variants, however, are stored in .uml file. The placements and replacements would have been defined for the variations in .uml file; the interactions of CHESS Modelling Language (CHESSML) compliant models with the BVR Tool are supported. The visual support for highlighting objects placements in red while replacements in blue colours, as well as retrieving selections are supported for Unified Method Architecture (UMA) metamodel and CHESSML compliant models.

3.1.2 Back-Propagation of Tailored Models. The execution of configuration/resolution generates the tailored model. The library contents are persisted in their own folders and XMI files; therefore the source code is altered for the adaptation of target location. The tailored models are automatically exported back to the desired locations in which the changes for resolving problems in XMI files and supporting the communication with realization editor had been reverted back. Tailored models are made available in EPF library that can be opened and visualized.

When the model variants are removed from the .uml file, the dangling stereotypes problem is caused. In particular, the repair stereotypes dialog pops up after the removal of model variants. To resolve this problem, the stereotypes applied at the placement variants are retrieved and deleted. Besides the dangling stereotypes, the orphan views appear in the diagram editors. In this context, the implemented command for clean diagrams needs to be executed; the style information of orphan views is removed from the .notation file. This is done for both opened and closed diagrams. The replacements in executed fragments have also been recorded. Specifically, the replacement variants are tracked within the .uml file and dropped at the diagram editors. After that, the Arrange All command is executed for the diagram editors.

3.2 Supporting the Change Impact Analysis in Process-Product Lines

In order to support the change impact analysis in process and product lines, the cross-cutting constraints (Section 3.2.1), joining of resolutions (Section 3.2.2) and simultaneous execution of multiple base models (Section 3.2.3) have been taken into consideration.

3.2.1 Enforcement of Cross-Cutting Constraints. The process and product variability might be specified in the combined or otherwise individual models. In the combined models, the individual branches might be taken into consideration. The constraints are enforced over the model elements, for which their names are considered. It is therefore important to avoid duplicates; the occurrences can also be defined. However, the BVR Tool support constraints for the current model elements.

The idea with the individual models is separation of concerns, so that the process engineers and product designers work on their respective models. The interactions between process and product models have been supported; the logical operators such as implication, alternative, negation might be used in the cross-cutting constraints. It is a meaningful way to enforce the process-product dependencies. There is also a need to consider the occurrence specifications between the variability models of a project. The presence of elements mentioned within the constraint is first checked in the current model. If the elements are not detected, the search is extended to other models in a project. In case the elements are detected in another model, the dialogue window pops up to inform the existence in specific model. The user, however, needs to authenticate the enforcement of cross-cutting constraints.

3.2.2 Joining of Variability Resolutions. The resolution editor is used for specification, validation and execution of process and product configurations. The resolutions are automatically generated from the VSpec model in which the varying choices needed to be included or excluded. It is possible to define multiple resolutions for the processes and products with variabilities. The constraints are used to specify the dependencies between choices. Therefore, there is a need to pair the process and product resolutions to perform error checking and validation. The validity of process-product impact analysis and change propagation is guaranteed if the cross-cutting constraints are properly specified.

3.2.3 Simultaneous Execution of Base Models. To be able to support the variant management and change impact analysis in

integrated lines, the execution of two or more base models is needed. A dialogue wizard is used to inform the possible candidates to the user, in particular, the models for which realization fragments have been specified. The checklist selection is supported for the base models. Besides that, the user either selects the execution of cross-cutting dependencies for the purpose of impact propagation, or otherwise the whole joined resolution is taken into consideration. Accordingly, the back-propagation of tailored models is performed. At the opening of EPF Composer and CHESS Toolset, the dialogue window pops up to inform that "the files have been changed on the file system. Do you want to load the changes?" Pressing the "Yes" button loads the tailored model(s). The support for saving the copy of previous models is also incorporated.

4 ILLUSTRATIVE SCENARIOS

This section discusses the tailoring scenarios of the attitude and orbit control subsystem. This system is used in a number of different telecommunication satellite platforms: the attitude control manages the orientation of the satellite, whereas the orbit control regulates the positioning of the satellite in orbit. Due to the large variety of space missions, performance and functional specifications, and the industrial organizations, the specified requirements tend to be tailored to the individual situations.

4.1 Establishment and Integration of Process and Product Lines

The ECSS-E-ST-40C [1] standard is applicable to the extent defined by the tailoring process, for instance, to all the elements of a space system, including the space segment, the launch service segment and the ground segment. It is however recommended that some requirements must not be tailored out, such as the production of a minimum set of software requirements, a preliminary design review, the production of the code, a validation against requirement and an acceptance. The assignment of criticality classification can make the requirements applicable, not applicable, or applicable under the certain conditions. The ECSS-E-ST-40C [1] and ECSS-Q-ST-80C [2] standards require the assignment of criticality classification based on the severity of potential consequences. The tailoring of particular standards is defined by considering the four criticality classifications of software products: catastrophic (A); critical (B); major (C); and minor or negligible (D). These standards are combined to specify all processes for space software development.

The attitude and orbit control subsystem consists of multiple modes, which might have different criticality classifications. The normal mode is used for the spacecraft purpose, for example, to support scientific observations. But, the safe mode is used for the initial acquisition and in case of contingencies. The normal mode is perceived as minor or negligible (D); whereas the safe mode is critical (B). The safety critical softwares (such as, safe mode) shall be designed, integrated, tested and validated independently from the rest of the softwares. The ECSS-E-ST-60-30C [3] standard presents the attitude and orbit control subsystem requirements. The selection of control methods is based on the operational environment of the satellites. Due to the strong magnetic fields, there is a need to control the torque disturbances in the low earth orbit satellites. The magnetic torques, however, provide the means to alter the system's angular momentum. This is not applicable to the satellites operating at much higher altitudes, such as geosynchronous orbit.

The requirement concerning the software detail design method states that the supplier shall use a design method (for example, object oriented or functional) to produce the design including software units, their interfaces and relationships. The selection of object oriented method is constrained with the product design in CHESS Toolset, as illustrated in Figure 2. The other alternatives, such as functional design with Simulink and the complexity might also be taken into consideration. The customer derives the performance and functional specifications of the software and hardware. The performance requirements, such as misalignment, noise and bias have been linked with the corresponding components that are grouped under processing. Another requirement states that the hardware and software designs must be consistent. If the hardware components are present, the resolutions shall consider the requirements for hardware characteristics, operating software, and environmental conditions. The CHESS Toolset supports in modelling the software and hardware, as well as the allocation of hardware to software. As per another process requirement, there is a need to enforce the automatic code generation with a tool from a model. Currently, the CHESS Toolset supports the generation of Ada source code. Besides the requirements, the criticality applicability of products is taken into consideration for the generation of corresponding processes.

4.2 Process-Product Impact Propagation

To generate the process and product models for the attitude and orbit control subsystem, the resolution is executed. Before that, the cross-cutting dependencies have been validated. The complete variations in the paired resolution are executed for the achievement of product and its process. The configured models are automatically exported back to the EPF Composer and CHESS Toolset.

5 CONCLUSIONS AND FUTURE WORK

Motivated by the need to perform the variant management and change impact analysis in process and product lines, the central theme of this paper focuses on two particular objectives: (i) the integration between EPF Composer, CHESS Toolset and BVR Tool is achieved; and (2) the process and product lines are integrated for which cross-cutting constraints between the variability models, joining of resolutions and simultaneous execution of realization fragments are taken into consideration. The impact propagation is either performed, or otherwise the complete variations in a paired resolution are executed. The tailored models are made available in EPF library and CHESS project that can be opened and visualized. The application of the proposed approach is illustrated for the attitude and orbit control subsystem. As future work, we plan to extend the integration to Polarsys OpenCert Tool[4] for assurance case variability in order to support variability management along three dimensions: process, product and assurance case.

ACKNOWLEDGMENTS

This work is supported by EU and VINNOVA via the ECSEL Joint Undertaking under grant agreement No. 692474, AMASS project.

[4] https://www.polarsys.org/opencert/

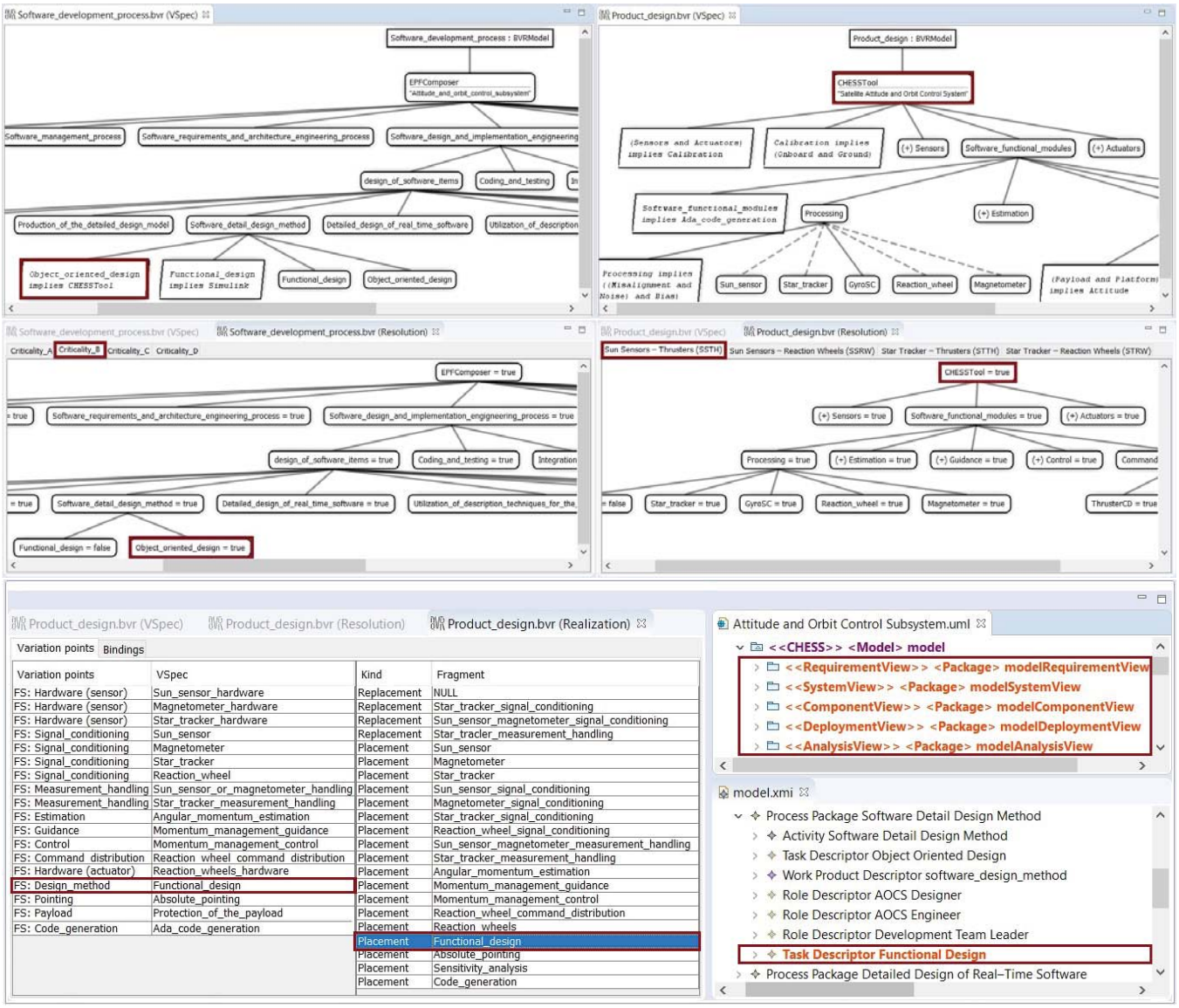

Figure 2: Integrated Process-Product Lines for the Attitude and Orbit Control Subsystem

REFERENCES

[1] European Cooperation for Space Standardization (ECSS). 2009. ECSS-E-ST-40C, Space Engineering – Software. (March 2009).

[2] European Cooperation for Space Standardization (ECSS). 2009. ECSS-Q-ST-80C, Space product assurance – Software product assurance. (March 2009).

[3] European Cooperation for Space Standardization (ECSS). 2013. ECSS-E-ST-60-30C, Space engineering – Satellite attitude and orbit control system (AOCS) requirements. (August 2013).

[4] Barbara Gallina. 2015. Towards Enabling Reuse in the Context of Safety-Critical Product Lines. In *5th IEEE/ACM International Workshop on Product Line Approaches in Software Engineering (PLEASE '15), Florence, Italy, May 19, 2015.*

[5] Muhammad Atif Javed and Barbara Gallina. 2018. Get EPF Composer back to the future: A trip from Galileo to Photon after 11 years. In *EclipseCon, Toulouse, France, JUNE 13-14, 2018.*

[6] Muhammad Atif Javed and Barbara Gallina. 2018. Safety-oriented process line engineering via seamless integration between EPF composer and BVR tool. In *Proceeedings of the 22nd International Systems and Software Product Line Conference (SPLC '18), Gothenburg, Sweden, September 10-14, 2018.*

[7] Andrzej Kobylinski. 2013. The Relationships between Software Development Processes and Software Product Quality. In *Proceedings of the 12th International Conference on Perspectives in Business Informatics Research (BIR '13), Warsaw, Poland, September 23-25, 2013.*

[8] Silvia Mazzini, John M. Favaro, Stefano Puri, and Laura Baracchi. 2016. CHESS: an Open Source Methodology and Toolset for the Development of Critical Systems. In *Joint Proceedings of the 12th Educators Symposium (EduSymp '16) and 3rd International Workshop on Open Source Software for Model Driven Engineering (OSS4MDE '16), Saint Malo, France, October 3, 2016.*

[9] Christian Prause, Markus Bibus, Carsten Dietrich, and Wolfgang Jobi. 2015. Tailoring process requirements for software product assurance. In *Proceedings of the 2015 International Conference on Software and System Process (ICSSP '15), Tallinn, Estonia, August 24 - 26, 2015.*

[10] Anatoly Vasilevskiy, Øystein Haugen, Franck Chauvel, Martin Fagereng Johansen, and Daisuke Shimbara. 2015. The BVR tool bundle to support product line engineering. In *Proceedings of the 19th International Conference on Software Product Line (SPLC '15), Nashville, TN, USA, July 20-24, 2015.*