Safety-critical Human- and Data-centric Process Management in Engineering Projects*

Cristina Cabanillas[1], Jan Mendling[1], Axel Polleres[1], and Alois Haselböck[2]

[1]Vienna University of Economics and Business, Austria {name.surname}@wu.ac.at
[2]Siemens AG Österreich, Corporate Technology, Vienna, Austria
alois.haselboeck@siemens.com

Abstract. Complex technical systems, industrial systems or infrastructure systems are rich of customizable features and raise high demands on quality and safety-critical aspects. The activities to create complete, valid and reliable planning and customization process data for a product deployment are part of an overarching engineering process that is crucial for the successful completion of a project and, particularly, for verifying compliance to existing regulations in a distributed, heterogeneous environment. In this paper, we discuss the challenges that process management needs to address in such complex engineering projects, and present an architecture that comprises the functionality required together with findings and results already obtained for its different components.

Keywords: Adaptation, compliance, engineering, process management, resource management, unstructured data

1 Introduction

Deployments of technical infrastructure products are a crucial part in the value-creation chain of production systems for large-scale infrastructure providers. A challenge is the management and monitoring of complex, yet mostly informally described, engineering processes that involve loosely integrated components, configurators and software systems [1]. The SHAPE project explores this domain in order to help engineers in the design, verification and configuration of complex systems. In particular, it aims at developing ICT support for more rigorous and verifiable process management in such recurring and adaptive engineering processes to face needs with respect to the formalization of process models, the integration of heterogeneous data sources, compliance checking automation and adaptability.

In this paper, we describe the challenges we identified for developing the required ICT support and present a solution approach as well as initial results already obtained in the scope of the project. Specifically, the rest of the paper is organized as follows. Section 2 delves into the problem and the challenges. Section 3 presents a conceptual solution and the current status of its development. Finally, Section 4 summarizes the ideas and outlines future work.

* This work is funded by the Austrian Research Promotion Agency (FFG) under grant 845638 (SHAPE): http://ai.wu.ac.at/shape-project/

2 Problem Description

An example of a large-scale, complex engineering process in a distributed and heterogeneous environment is the construction of a railway system comprising electronic interlocking systems, European train control systems, operator terminals, railroad crossing systems, etc.; all of them are available in different versions and technologies. It is necessary to offer, customize, integrate, and deliver a subset of these components for a particular customer project, e.g., the equipment of several train stations with an electronic switching unit in combination with a train control system based on radio communication for a local railway company. Configurators are engineering tools for planning and customizing a product. Each subsystem comes with its own, specialized engineering and verification tools. Therefore, configuring and combining these subsystem data to a coherent and consistent system has to follow a complex, collaborative process. Studying this process in a real setting, the following challenges have been identified:

Challenge 1: Integrated description of processes, constraints, resources and data. Several formal languages are at hand for describing processes, constraints, resources and data separately, but no integrating model exists that provides such rich querying functionality to support status monitoring or, respectively, the verification of constraints and consistency w.r.t. compliance rules and regulations.

Challenge 2: Integration and monitoring of structured and unstructured data. To a high degree, engineering steps are the input for state changes of the process, often only visible as manipulation of data. To this end, various types of systems have to be integrated including their structured and unstructured data (e.g., by mail traffic, or ticketing systems). Up until now, these data are hardly integrated and monitored mostly manually.

Challenge 3: Documentation of safety-critical aspects. Engineering projects have time-critical phases typically prone to sloppy documentation and reduced quality of results. Many of the process steps are required to be documented in prescribed ways by standards and regulations (e.g., SIL [2]). The semi-automatic mapping of witnessing data and the deployment of a Business Process Management Systems (BPMS) would help in compliance checking with such regulations.

Challenge 4: Be ready for changes. Monitoring the engineering activities and applying appropriate process patterns may lead to modification proposals of the process to make it simpler and less error-prone. Currently, these adaptations require manual work and are prone to errors.

Challenge 5: Acceptance and human factors. The overall process management needs to be set up in a non-obtrusive way, such that engineers executing the processes find it useful and easy to use. This is a specific challenge in safety-critical systems, which are developed with a tight timeline. It calls for a design that integrates existing tools and working styles instead of introducing new systems.

3 Solution Approach

In order to address the challenges mentioned in Section 2, we propose the conceptual solution depicted in Fig. 1, which includes the following functionality:

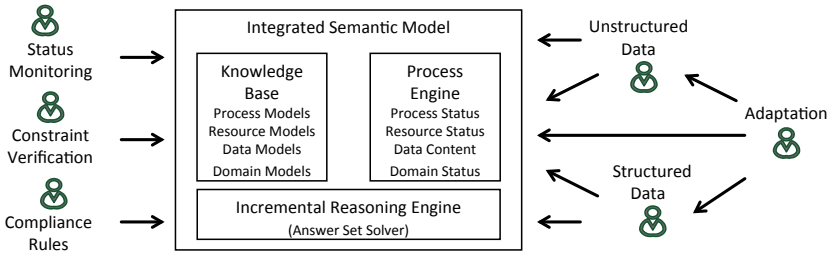

Fig. 1: Sketch of the solution

An integrated semantic model to describe and monitor processes, resources, constraints and data. The model shall be integrated with existing process engines, but allows for more rigorous monitoring of resource and data flow constraints at the process instance level. *Status:* We have developed an engineering domain ontology [3] that represents: (i) engineering domain and organizational (i.e, resource-related) knowledge; (ii) business processes; and (iii) regulations and policies [4]. On top of the knowledge base, we have developed an approach to automate the allocation of resources to process activities based on the reasoning formalism Answer Set Programming (ASP) [5], which we plan to extend in several directions, e.g., to integrate calendar information or to consider various resource and domain constraints (with the focus on safety-related constraints).

Mechanisms to detect and extract structured from unstructured process data. Existing methods from the domain of natural language processing and ontology learning can be used to this end. *Status:* We have developed an approach to mine project-oriented business processes from version control system data that analyses the commits stored in the logs to derive Gantt charts describing the project activities [6]. Furthermore, we have extended the scope of traditional process mining approaches (focused on control flow) to extract resource assignment rules, a.o. [7]. Extensions are being developed for both approaches.

Domain-specific models using the integrated description formalism. This includes regulations and legal compliance rules that help to document safety-critical aspects of systems and processes. *Status:* We have studied specific norms in the railway domain and we have translated the process-relevant unstructured descriptions into semi-structured data that we plan to use to add compliance information to the process models in order to ease compliance checking at process execution time [8]. Next steps in this regard comprise mining the semi-structured rules and representing them with the engineering domain ontology.

Flexibility, adaptability and robustness. Methods to deal with changes (e.g., reconfigure resources w.r.t. changed processes) must be put in place. *Status:* We aim to develop flexible approaches that allow for adding new functionality while using well-tested methods to ensure robustness. We are currently collecting relevant adaptation requirements from rail automation and studying existing process adaptivity mechanisms that involve control flow [9], data [10] and resources [11].

Validation of the results. The solution has been designed to be evaluated in a real-world setting in the railway domain. *Status:* We have designed an archi-

tecture [12] that includes the aforementioned functionality, namely, executable process models, adaptation procedures and procedures for process mining to ensure continuous enhancement. It will be integrated into the Camunda[1] BPMS.

4 Conclusions and Future Work

This paper summarizes the first findings and results for safety-critical human- and data-centric process management in engineering projects. We are exploring existing techniques (e.g., text mining and resource allocation approaches) that can be integrated with our approaches to extend the current support. Next steps also involve putting in place adaptation mechanisms, implementing and integrating all the components into Camunda, and conducting a thorough evaluation of the respective components w.r.t. real data from the railway domain.

References

1. G. Fleischanderl, G. E. Friedrich, A. Haselböck, H. Schreiner, and M. Stumptner, "Configuring Large Systems Using Generative Constraint Satisfaction," *IEEE Intelligent Systems*, vol. 13, no. 4, pp. 59–68, 1998.
2. M. Bozzano and A. Villafiorita, *Design and safety assessment of critical systems*. CRC Press Taylor & Francis Group, 2010.
3. C. Cabanillas, A. Haselböck, J. Mendling, A. Polleres, S. Sperl, and S. Steyskal, "Engineering Domain Ontology." SHAPE project deliverable.
4. S. Steyskal and A. Polleres, "Defining expressive access policies for linked data using the ODRL ontology 2.0," in *SEMANTICS 2014*, pp. 20–23, 2014.
5. G. Havur, C. Cabanillas, J. Mendling, and A. Polleres, "Automated Resource Allocation in Business Processes with Answer Set Programming," in *BPM Workshops (BPI)*, p. In press, 2015.
6. S. Bala, C. Cabanillas, J. Mendling, A. Rogge-Solti, and A. Polleres, "Mining Project-Oriented Business Processes," in *BPM*, pp. 425–440, 2015.
7. S. Schönig, C. Cabanillas, S. Jablonski, and J. Mendling, "Mining the Organisational Perspective in Agile Business Processes," in *BPMDS*, pp. 37–52, 2015.
8. J. Fuchsbauer, "How to manage Processes according to the European Norm 50126 (EN 50126)." Bachelor thesis, 2015.
9. R. Conforti, M. Dumas, M. L. Rosa, A. Maaradji, H. Nguyen, A. Ostovar, and S. Raboczi, "Analysis of Business Process Variants in Apromore," in *BPM Demos*, pp. 16–20, 2015.
10. D. Müller, M. Reichert, and J. Herbst, "A New Paradigm for the Enactment and Dynamic Adaptation of Data-Driven Process Structures," in *CAiSE*, vol. 5074, pp. 48–63, 2008.
11. S. Rinderle-Ma and M. Leitner, "On Evolving Organizational Models without Losing Control on Authorization Constraints in Web Service Orchestrations," in *CEC*, pp. 128–135, 2010.
12. T. B. Ionescu, "Architecting Semantic Process Mining-Driven Optimization and Adaptation of Business Workflows for the Mobility Industry," in *SEMANTICS 2015*, p. In press, 2015.

[1] `http://camunda.org/`