Towards Trustworthy Adaptation of Cyber-Physical Production Systems with Contract-Based Design

Hossein Rahmani[†] Kristof Meixner[†] Stefan Biffl[†]
[†]Institute of Information Systems Engineering, TU Wien
E-Mail: [first].[last]@tuwien.ac.at

Abstract—**Adapting a Cyber-Physical Production System (CPPS) to different production goals and conditions requires capabilities to validate multi-domain dependencies. Traditional approaches to CPPS adaptation rely on domain experts' implicit knowledge, making reconfiguration prone to error, challenging to validate, and hard to trust. Our research aims at improving the trustworthiness of the CPPS adaptation process regarding effectiveness, risk mitigation, and understandability, with a formal representation of reconfiguration dependencies and conditions. This paper introduces the approach *Trustworthy Adaptation Process for CPPS (TAP-CPPS)* to validate the feasibility of achieving the adaptation goal by reconfiguration. TAP-CPPS is a systematic approach to (i) model the adaptation process using BPMN; and (ii) validate the adaptation process model using *contracts* by verifying explicit reconfiguration pre-/post-conditions in the BPMN model, which is linked to the CPPS configuration variants. We initially evaluate TAP-CPPS with a use case of a CPPS for joining car parts, and derive a research agenda.**

Index Terms—**Production Systems Engineering, Industry 4.0, Multi-disciplinary reconfiguration, Adaptive production system.**

I. Introduction

Industry 4.0 (I4.0) has envisioned to realize adaptive Cyber-Physical Production Systems (CPPSs) [1] in order to meet the growing demands for flexible and responsive production [2]. In this work, CPPS adaptation refers to the process of adjusting the CPPS's behavior in response to a change in a dynamic production environment [3]. An adaptation process often involves reconfiguring several components, including Product-Process-Resource (PPR) aspects, to achieve the *target adaptation goal*, such as addressing changes in market demands and customer requirements [4], technology [5], or regulations [3], [6].

Traditional approaches for CPPS adaptation and reconfiguration [7] rely on domain experts' implicit knowledge. This tacit knowledge is often fragmented among experts coming from several domains, e.g., mechanical, electrical, system, and software engineering, each of whom has partial or incomplete knowledge required for designing and evaluating adaptation. Hence, traditional CPPS adaptation approaches are prone to error, challenging to validate, and hard to trust [5], [8].

Considering the complex multidisciplinary nature of a CPPS and its adaptation process, structured methods and appropriate models are required to enhance the *trustworthiness of CPPS adaptation* and the underlying reconfigurations [1], [5], [8]. Trustworthiness is an umbrella term for properties including safety, security, reliability, integrity, availability, and understandability [9]–[11]. This work focuses on the integrity and understandability aspects of trustworthiness.

To address the challenges and enhance the *trustworthiness of CPPS adaptation*, this paper proposes a systematic multi-view approach to ensure (i) the target configuration variants are valid; (ii) the target adaptation goal is achievable by the planned reconfigurations; and (iii) the adaptation and reconfiguration processes are understandable and verifiable by humans (various stakeholders) and machines. This paper shall address the Research Question: *What approach can validate whether a target adaptation goal is achievable by planned reconfiguration activities?*

With this aim, we introduce the approach *Trustworthy Adaptation Process for CPPS (TAP-CPPS)* built on the approach *PPR Asset Network with Reconfiguration (PAN+R)* [5]. TAP-CPPS is a systematic approach to (i) model the CPPS adaptation process using the Business Process Model and Notation (BPMN); and (ii) validate the adaptation process model and underlying reconfigurations using *contracts* [12] by explicitly verifying the reconfiguration pre- and post-conditions in the BPMN, which is linked to the CPPS configuration variants.

We illustrate an application of TAP-CPPS to evalutate the reconfiguration of an automated industrial screwdriver, a typical flexible resource in car production.

The remainder of this paper is structured as follows. Section II summarizes the related work. Section III introduces the use case. Section IV introduces our proposed approach, TAP-CPPS, illustrated with data from the use case. Finally, Section V concludes the paper with a research agenda.

II. Related Work

Multi-view Configuration Management (CM) in CPPS engineering, according to the VDI 3695 [7], aims at managing the correct migration between CPPS configurations. A CPPS configuration represents a consistent, validated combination of all required system elements. While the VDI 3695 addresses multidisciplinary CM, it does not address trustworthy CM.

The guideline VDI 3682 [13] provides a formalism for describing the production processes based on the core PPR concepts. Building on PPR, the *PPR Asset Network (PAN)* [14] is an I4.0 asset-based coordination artifact, which can represent PPR dependencies for a specific configuration variant. However, it does not support multiple variants required for reconfiguration. Extending the PAN, the *PAN+R* approach [5] provides (i) knowledge representation required to coordinate CPPS reconfiguration, and (ii) an approach for validating the reconfiguration process based on multidisciplinary pre-

Manuscript received July 15, 2025; revised July 31, 2025; accepted July 25, 2025. Published September 2, 2025.
Issue category: Special Issue on DSD/SEAA 2025 on Works in Progress (WiP) Session, Salerno, Italy, Sept. 2025
Paper category: Short
DOI: doi.org/10.64552/wipiec.v11i1.87

and post-conditions. However, the PAN+R does not consider formal notations for modeling complex adaptation processes.

Trustworthy adaptation of CPPS requires a suitable architecture that supports the modeling and management of multi-domain reconfiguration knowledge and coordination of the adaptation process [15]. MAPE-K [16] defines a reference framework for self-adaptive systems by organizing the adaptation process into four core functions: Monitor, Analyze, Plan, and Execute, along with a central Knowledge component. MAPE-K encourages the principle of separation of concerns, which provides a suitable basis for our proposed approach.

The BPMN standard [17] allows modeling complex business processes that technical and non-technical experts, and machines can interpret. The BPMN can be used to extend the PAN+R approach for modeling complex adaptation processes. Yet, BPMN *per se* does not consider PPR assets or the conditions and data required for the adaptation validation. This work explores linking the adaptation process in BPMN to PPR assets and conditions [5], [18] using *contracts* [12].

A contract for a component is a pair of an assumption and a guarantee. The component guarantees a particular behavior if the environment satisfies the assumption [12]. Contract-based design is a rigorous method for verification, analysis, and abstraction/refinement [12], However, to our knowledge, this method has not been applied to adaptive CPPSs.

The modeling method *procan.do* [19], [20] facilitates understanding, for a process or system of interest, the assets, stakeholders, and data required to analyze multi-domain contributions to a desired or undesired outcome. In this paper, we use procan.do to derive the stakeholders, contract conditions, and data sources required to evaluate the contract conditions.

This paper shall go beyond the state of the art in CPPS adaptation and reconfiguration [5], [7]. We introduce a systematic multi-view approach to validate whether the target adaptation goal is achievable by the planned reconfiguration activities.

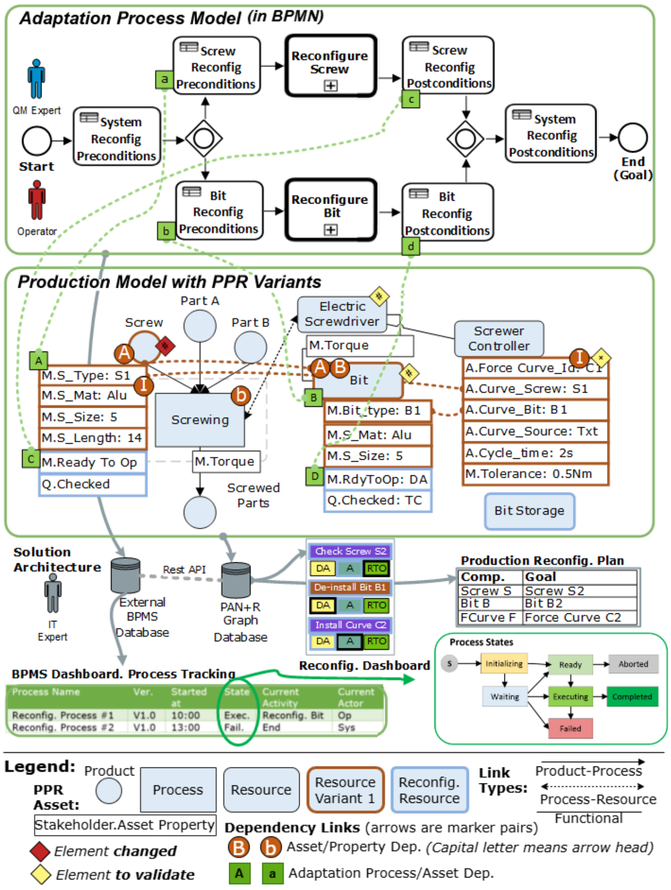
III. Use Case Work Cell Adaptation

Based on a domain analysis of screwing work cells [21], [22], we abstracted the illustrative use case *adaptation of a screwing work cell*. Moreover, we identified the requirements for knowledge representation on reconfiguration. Specifically, we describe components of a robotic work cell equipped with an electric screwdriver. The screwdriver consists of a bit and a screwer controller that uses a force curve to define the screwing process behavior.

In the use case, a quality expert collaborates with process experts and detail planners to define and validate reconfiguration procedures for the operator who conducts the reconfiguration. A representative multidisciplinary reconfiguration task is changing the screw type. This change requires checking and modifying the screwing bit and the force curve of the screwing process. It involves dependencies between all PPR aspects, including mechanical and automation engineering disciplines. For validating a reconfiguration process with PPR change dependencies, we identified three essential modeling requirements: (R1) representation of the PPR change knowledge, (R2) representation of the reconfiguration process, and (R3) linking the reconfiguration process with the PPR model, making dependencies explicit for validation and traceability.

IV. Trustworthy Adaptation Process for CPPS

This section introduces the approach *Trustworthy Adaptation Process for CPPS (TAP-CPPS)* and demonstrates its application using data from the use case *adaptation of a screwing work cell*. We apply *procan.do* [19], [20] to analyze dependencies in the adaptation process. We identify the assets, stakeholders, conditions, and data sources required to evaluate, verify, and validate *contracts* [12] in the adaptation process.



Comp.	Goal
Screw S	Screw S2
Bit B	Bit B2
FCurve F	Force Curve C2

Process Name	Ver.	Started at	State	Current Activity	Current Actor
Reconfig. Process #1	V1.0	10:00	Exec.	Reconfig. Bit	Op
Reconfig. Process #2	V1.0	13:00	Fail.	End	Sys

Fig. 1. *Trustworthy Adaptation Process for CPPS (TAP-CPPS) approach*: Solution Overview.

Fig. 1 illustrates the TAP-CPPS approach consisting of (i) a *Production Model with PPR variants* and the required production change knowledge (cf. Fig. 1, middle), (ii) an *Adaptation Process Model* including the required reconfiguration knowledge (cf. Fig. 1, top), and (iii) *Links between the adaptation process elements and the production assets* (cf. Fig. 1, green dashed lines) for validating the reconfiguration pre- and post-conditions (cf. Tab. I) using contracts. These linked models form a knowledge graph that can be queried to (i) derive and validate an adaptation plan with the underlying reconfigurations, and (ii) inform the operators via a dashboard about the reconfiguration tasks and their current status. The main parts of TAP-CPPS (cf. Fig. 1) are explained as follows.

(i) Production Model with variants. The TAP-CPPS production model builds on the PAN [14] to represent PPR assets and properties (circles and boxes in light blue color), such as the screwing process and functional dependencies between PPR assets (black arrows). The production model also contains variants of the PPR assets and properties (PPR elements with frames in brown color) to represent the production variants, such as screw types, bits, screwing processes, and screwing force curves. The variants of a PPR element are connected by transition dependencies (brown arrows with dashed lines). The change dependencies between (variants of) PPR elements are also represented in the production model by brown dashed lines, e.g., between the screw and the bit.

TAP-CPPS production model properties can represent the reconfiguration states of components, such as *assembly* or *validation* states. For validating a sequence of reconfiguration tasks, the valid states and transitions can be defined using state machines, considering multidisciplinary dependencies. To represent reconfiguration assets or properties required only for coordinating the adaptation, not for production, the production model contains PPR elements in a light blue frame, e.g., *Bit Storage*. The production model uses red and yellow diamonds for marking a changed PPR asset and the related PPR elements to validate. The validation of each element can be addressed by a *contract*, defined as a set of *assumption* pre-conditions and a set of *guarantee* post-conditions, and its evaluation process.

(ii) Adaptation Process Model. An adaptation process consists of reconfiguration tasks with pre- and post-conditions, each leading from a start to a goal state (cf. Fig. 1, top). For instance, the adaptation of the screwing system requires reconfiguration tasks for the screw, bit, and screwing curve. The process expert defines the reconfiguration task conditions considering dependencies and states in the TAP-CPPS production model. A Business Process Management System (BPMS) can track and monitor the execution of the adaptation process for normal or special cases.

(iii) Knowledge graph of the adaptation process linked to the production assets. The domain concepts in the task pre- and post-conditions linked to PPR elements (cf. Fig. 1, green dashed lines) build the foundation to validate these concepts with their dependencies in the TAP-CPPS knowledge graph using *contracts* [12] and an information system for validation.

Evaluation. As an initial feasibility evaluation, we conducted TAP-CPPS for the use case *adaptation of a screwing work cell* (cf. Section III) following the *procan.do* method.

Step 1: The scope of work is the adaptation of the screwing work cell (cf. Fig. 1) with desired and undesired outcomes.

Step 2: Process analysis results in a BPMN process model for adapting the screwing work cell with the required reconfiguration tasks (cf. Fig. 1, top). This adaptation model should lead to desired outcomes, such as completing the customer orders on time, with limited resources. This step identifies high-risk undesired process outcomes, such as completing the customer orders with delays or high unplanned costs.

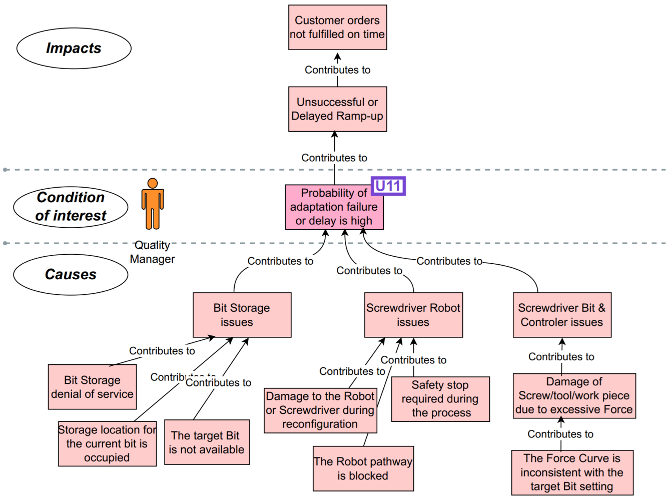

Impacts
Customer orders not fulfilled on time
Contributes to
Unsuccessful or Delayed Ramp-up
Contributes to
Condition of interest
Quality Manager
Probability of adaptation failure or delay is high
U11
Causes
Contributes to
Contributes to
Contributes to
Bit Storage issues
Screwdriver Robot issues
Screwdriver Bit & Controler issues
Contributes to
Bit Storage denial of service
Contributes to
Contributes to
Storage location for the current bit is occupied
The target Bit is not available
Contributes to
Contributes to
Damage to the Robot or Screwdriver during reconfiguration
Safety stop required during the process
The Robot pathway is blocked
Contributes to
Damage of Screw/tool/work piece due to excessive Force
Contributes to
The Force Curve is inconsistent with the target Bit setting

Fig. 2. Undesired conditions in adaptation process of *Screwing Work Cell*.

TABLE I
PRE- AND POST-CONDITIONS OF RECONFIGURATION TASKS (CF. FIG. 1).

Condition Id	Condition Description
Screw.Reconfig. Precondition	'Screw S1'.M.'Ready To Op' == assembled ∨ ready ∧ 'Screw S2'.M.'Ready To Op' == disassembled.
Screw.Reconfig. Postcondition	'Screw S2'.M.'Ready To Op' = assembled ∨ ready ∧ 'Screw S1'.M.'Ready To Op' == disassembled.
Bit.De-install Precondition	'Bit B1'.M.'Ready To Op' == assembled ∨ ready ∧ 'Bit B2'.M.'Ready To Op' == disassembled.

Step 3: Condition analysis starts with analyzing the desired conditions of the "sunshine case" in the BPMN model, coming from Step 2. Then, analysis shall focus on an undesired condition, e.g., *"probability of adaptation failure or delay is high"* (cf. Fig. 2). Domain experts shall identify conditions, including the pre- and post-conditions (cf. Tab. I) to be verified by *contracts* at interfaces between stakeholder modules.

Step 4: Analyze assets, stakeholders, and dependencies related to the conditions and identify the asset properties and data sources required to evaluate these conditions [20].

Step 5: Validate contract conditions evaluates for the steps in a reconfiguration process the fulfillment of pre- and post-conditions (cf. Tab. I) to list the issues, in particular, false post-conditions (guarantee) with true pre-conditions (assumption).

In the evaluation, we identified lines of undesired conditions likely to contribute to an undesired outcome (cf. Fig. 2). The combination of conditions can specify *special cases* that require countermeasures, which may be expressed as a contract for the expected behavior. In the use case context, the TAP-CPPS approach facilitated modeling the adaptation process in BPMN and validating contract conditions on the adaptation process for typical reconfiguration activities, which may result in *special cases*. Therefore, TAP-CPPS was found sufficient to validate the feasibility of the adaptation goal by stepping through typical reconfiguration chains of tasks.

V. Conclusion

The Industry 4.0 vision of adaptable robot work cells [23] requires capabilities for (i) multidisciplinary reconfiguration based on a model with PPR dependencies; (ii) the flexible design of reconfiguration processes according to a production model to accommodate for new products, processes, and production system components; and (iii) coordinating human and machine agents. However, traditional reconfiguration processes are (i) often workflows designed for a specific production system and (ii) unaware of production dependencies.

In this paper, we introduced the TAP-CPPS approach that goes beyond the state of the art [5], [7] by representing PPR asset dependencies in a production model. This representation facilitates validating a flexible reconfiguration process as a foundation for coordinating production reconfiguration. Together, the TAP-CPPS production model and the reconfiguration process model can represent the data required for change planning and monitoring. Further, the TAP-CPPS knowledge graph facilitates queries to PPR elements, their variants, and dependencies [14]. Thus, TAP-CPPS provides the basis for effective change coordination of human and machine agents. An initial evaluation of the TAP-CPPS knowledge graph using the screwing work cell use case showed promising results. This suggests exploring its application in a broader range of production adaptation settings that face trustworthiness challenges to better understand its strengths and limitations.

Overall, TAP-CPPS seems well suited to enhance the trustworthiness of the CPPS adaptation process by supporting the specification and validation of reconfiguration effectiveness and mitigating associated risks. It also offers a formal representation of PPR reconfiguration dependencies and conditions, making it suitable for auditing industrial production processes.

Research agenda. *Towards trustworthy self-adaptive production.* We plan to apply the TAP-CPPS approach for production system reconfiguration by coordinating (i) the PPR reconfiguration process design and validation regarding contracts on dependencies in and across disciplines; and (ii) one or more operators with tool support towards valid reconfiguration with run-time input data. We consider investigating (i) operator assistance with a reconfiguration dashboard (cf. Section IV); and (ii) automating selected reconfiguration tasks towards a self-adaptive CPPS for a suitable scope of reconfiguration.

Empirical studies. We plan to identify applicable metrics and explore the trustworthiness, usability and usefulness, and scalability of the TAP-CPPS approach with domain experts in empirical studies in various production adaptation contexts. Also, we plan to conduct quantitative evaluations to report the results of quantitative performance analysis for TAP-CPPS.

Scalability. We plan to explore how to derive a reconfiguration process from a TAP-CPPS production model for large use cases, such as a robot for flexible use in various work cells and lines that may require dozens of production dependencies and a dozen change variants to the robot configuration.

References

[1] T. Müller, B. Caesar, M. Weiß, S. Ferhat, N. Sahlab, A. Fay, R. Oger, N. Jazdi, and M. Weyrich, "Reconfiguration management in manufacturing: A systematic literature review," *at - Automatisierungstechnik*, vol. 71, no. 5, pp. 330–350, May 2023, literatur Review.

[2] R. Dumitrescu, T. Westermann, and T. Falkowski, "Autonome systeme in der produktion," *Industrie 4.0 Management*, pp. 17–20, 2018.

[3] D. Weyns, I. Gerostathopoulos, N. Abbas, J. Andersson, S. Biffl, P. Brada, T. Bures, A. Di Salle, M. Galster, P. Lago, G. Lewis, M. Litoiu, A. Musil, J. Musil, P. Patros, and P. Pelliccione, "Self-adaptation in industry: A survey," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 18, no. 2, pp. 1–44, May 2023.

[4] K. Meixner, F. Rinker, L. Waltersdorfer, A. Lüder, and S. Biffl, "Organizing reuse for production systems engineering with capabilities and skills: Organisation der wiederverwendung im engineering von produktionsystemen mit capabilities und skills," *at - Automatisierungstechnik*, vol. 71, no. 2, pp. 116–127, Feb. 2023.

[5] S. Biffl, K. Meixner, D. Hoffmann, J. Musil, H. Rahmani, and A. Luder, "Towards coordinating production reconfiguration," in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, Sep. 2022, pp. 1–4.

[6] A. Musil, J. Musil, D. Weyns, T. Bures, H. Muccini, and M. Sharaf, *Patterns for Self-Adaptation in Cyber-Physical Systems*. Springer International Publishing, 2017, pp. 331–368.

[7] *VDI Guideline 3695: Engineering of industrial plants - Eval. and opt.* Beuth, 2009.

[8] H. Haddou Benderbal, A. R. Yelles-Chaouche, and A. Dolgui, *A Digital Twin Modular Framework for Reconfigurable Manufacturing Systems*. Springer International Publishing, 2020, pp. 493–500.

[9] J. M. G. Sánchez, N. Jörgensen, M. Törngren, R. Inam, A. Berezovskyi, L. Feng, E. Fersman, M. R. Ramli, and K. Tan, "Edge computing for cyber-physical systems: A systematic mapping study emphasizing trustworthiness," *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 3, pp. 1–28, Jul. 2022.

[10] R. F. Babiceanu and R. Seker, "Trustworthiness requirements for manufacturing cyber-physical systems," *Procedia Manufacturing*, vol. 11, pp. 973–981, 2017.

[11] Z. Yu, L. Zhou, Z. Ma, and M. A. El-Meligy, "Trustworthiness modeling and analysis of cyber-physical manufacturing systems," *IEEE Access*, vol. 5, pp. 26 076–26 085, 2017.

[12] A. Benveniste, B. Caillaud, A. Ferrari, L. Mangeruca, R. Passerone, and C. Sofronis, *Multiple Viewpoint Contract-Based Specification and Design*. Springer Berlin Heidelberg, 2008, pp. 200–225.

[13] *VDI Guideline 3682 Formalised Process Descriptions.*, Beuth Verlag Std., 2015.

[14] S. Biffl, J. Musil, A. Musil, K. Meixner, A. Lüder, F. Rinker, D. Weyns, and D. Winkler, "An Industry 4.0 Asset-Based Coordination Artifact for Production Systems Engineering," in *Int. Conf. Busi. Inf.* IEEE, 2021.

[15] T. Müller, S. Kamm, A. Löcklin, D. White, M. Mellinger, N. Jazdi, and M. Weyrich, "Architecture and knowledge modelling for self-organized reconfiguration management of cyber-physical production systems," *International Journal of Computer Integrated Manufacturing*, vol. 36, no. 12, pp. 1842–1863, Sep. 2022.

[16] J. Kephart and D. Chess, "The vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003.

[17] Object Management Group, "Business Process Model and Notation (BPMN), Version 2.0," Object Management Group, Tech. Rep. formal/2011-01-03, Jan. 2011.

[18] H. Rahmani, S. Biffl, K. Meixner, D. Hoffmann, A. Lüder, and D. Winkler, "Business risk analysis of production variants considering technical dependencies," in *Int. Conf. Busi. Inf.* IEEE, Sep. 2024, pp. 178–187.

[19] Biffl, S., "Introduction to procan.do," QSE Technical Report QSE 2025-02, TU Wien, 2025.

[20] S. Biffl, S. Kropatschek, K. Meixner, D. Hoffmann, and A. Lüder, "Configuring and validating multi-aspect risk knowledge for industry 4.0 information systems," in *Int. CAiSE*. Springer, 2024, pp. 492–508.

[21] J. Herzog, H. Röpke, and A. Lüder, "Analysis of the reusability of modules in automotive assembly," in *IEEE ETFA*, 2021, pp. 1–8.

[22] K. Meixner, K. Feichtinger, R. Rabiser, and S. Biffl, "A reusable set of real-world product line case studies for comparing variability models in research and practice," in *Int. SPLC. Vol. B*. ACM, 2021.

[23] T. D. Thomas Bauernhansl, Manuel Fechter, *Entwicklung und Demonstration einer wandlungsfähigen Forschungsproduktion*. Springer, 2020.