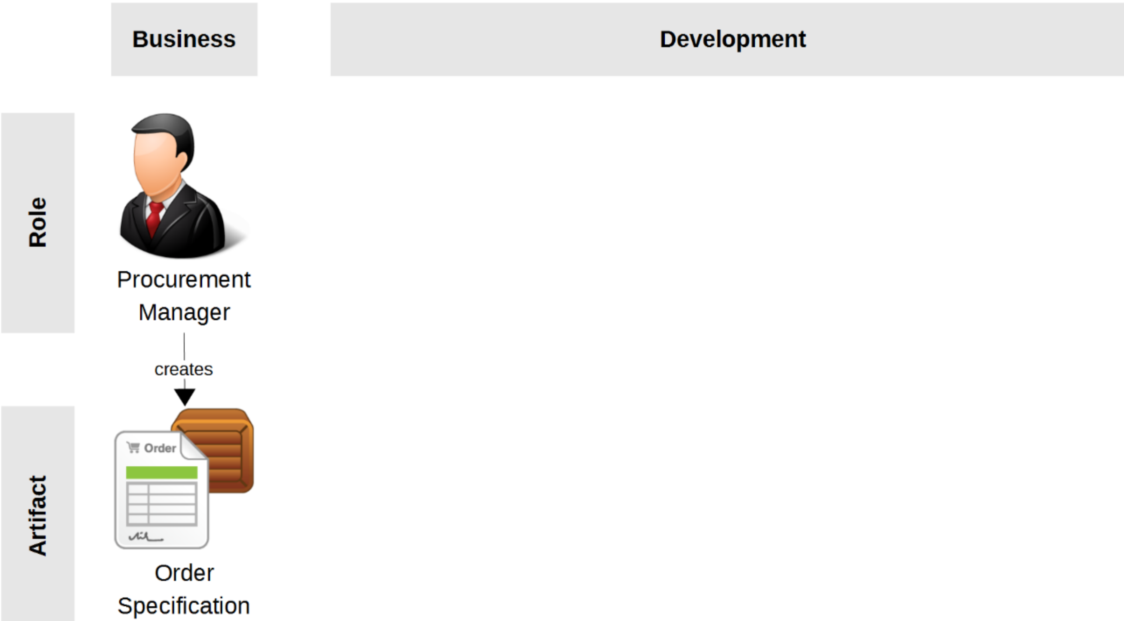
Formal Technical Process Specification and Verification for Automated Production Systems

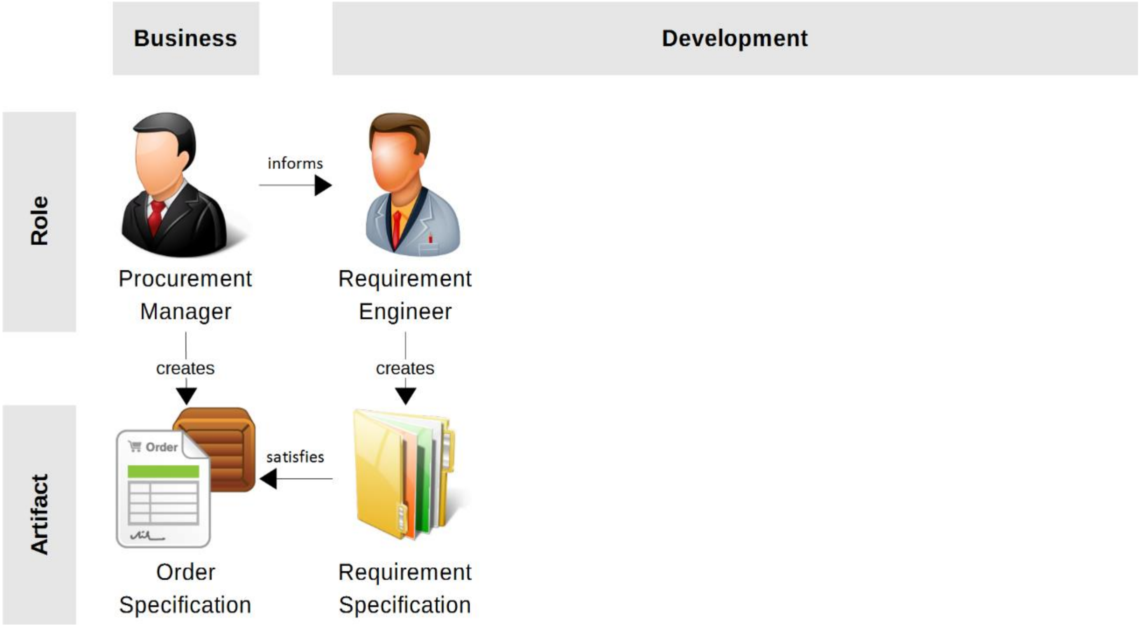
Georg Hackenberg, Alarico Campetelli, Christoph Legat,
Jakob Mund, Sabine Teufl and Birgit Vogel-Heuser

Motivation » Automated Production Systems (Google)

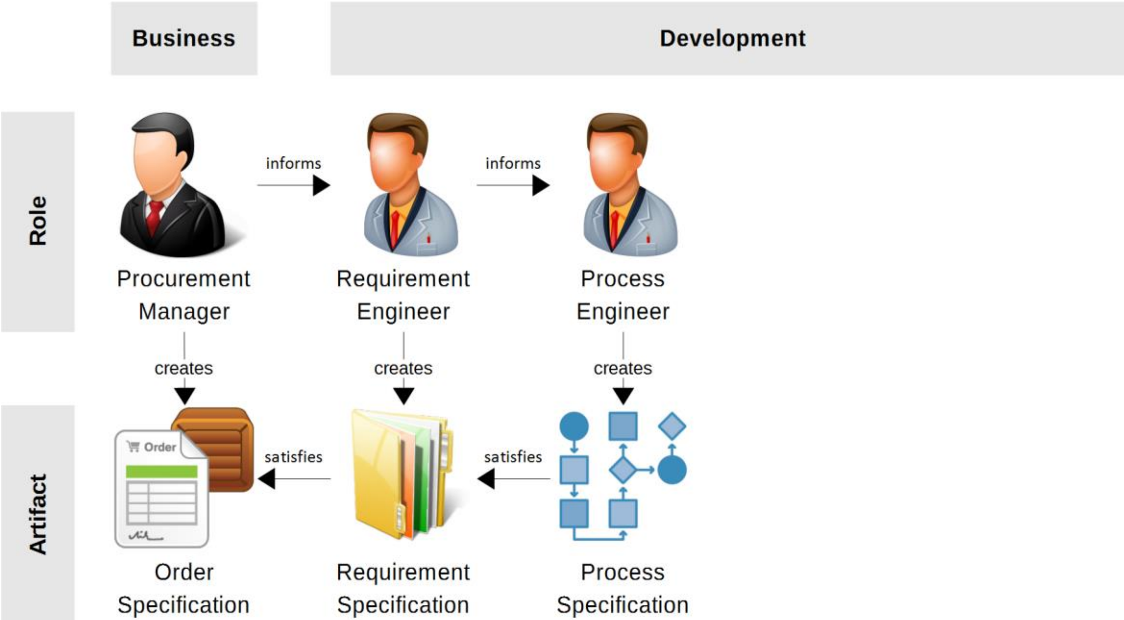
Motivation » Systems Development Process (Simple)



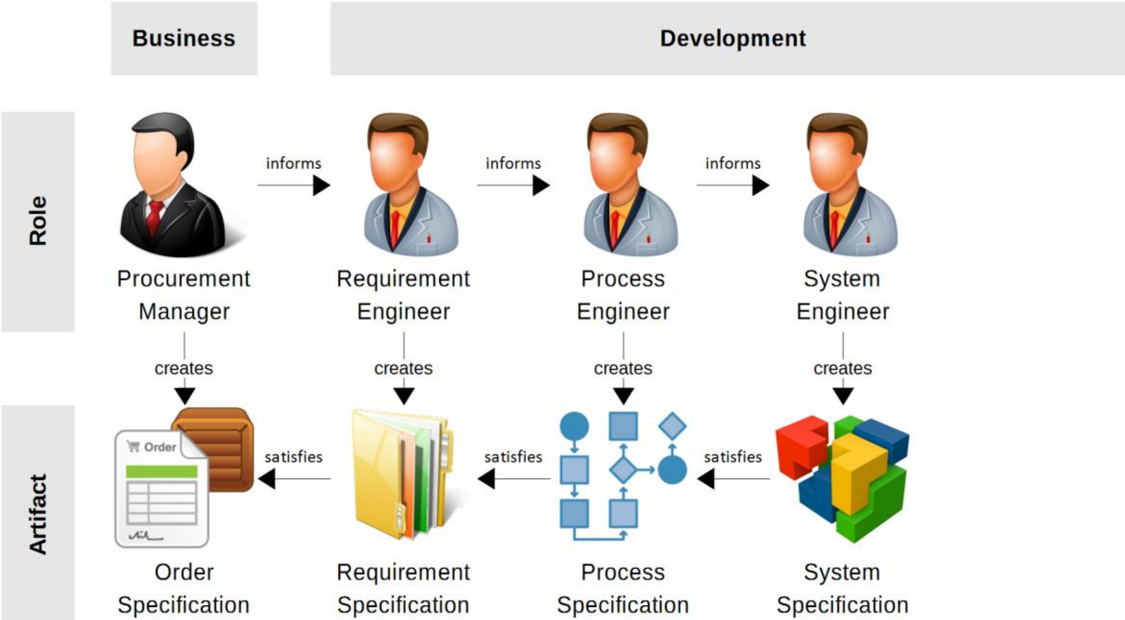
Motivation » Systems Development Process (Simple)



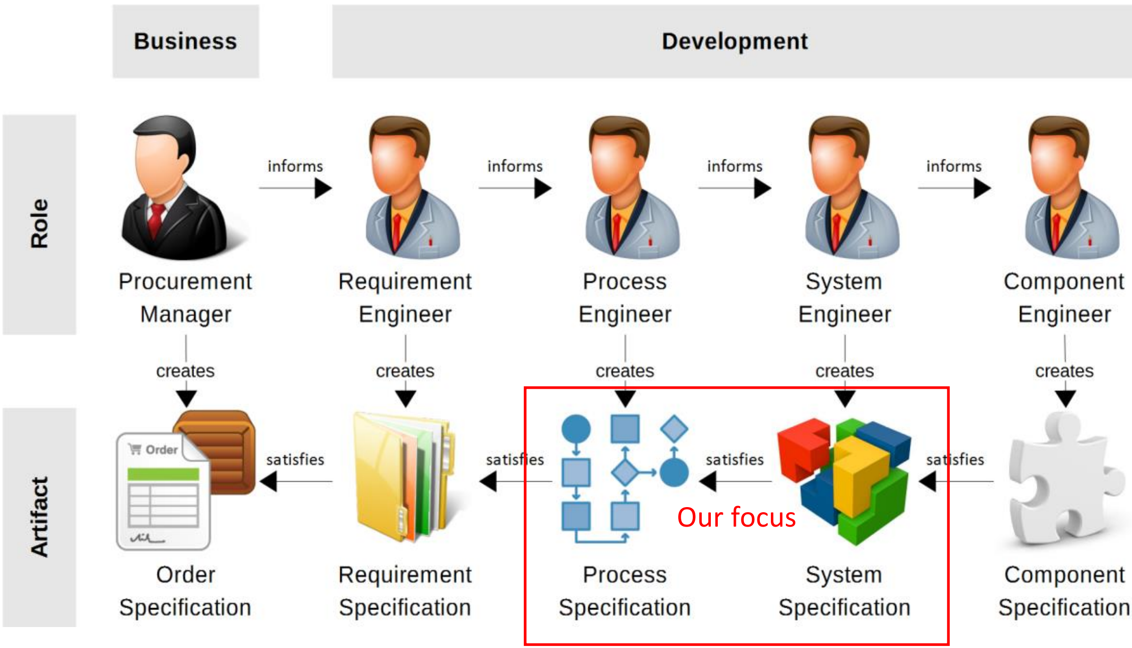
Motivation » Systems Development Process (Simple)



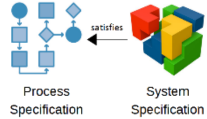
Motivation » Systems Development Process (Simple)



Motivation » Systems Development Process (Simple)



Motivation » State of the Art



Process Specification Techniques

– Business Process Model & Notation

– Formalized Process Description

But what we found missing is …

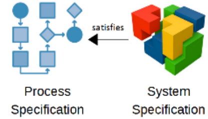
a general integrated approach to process specification and design / run time verification.

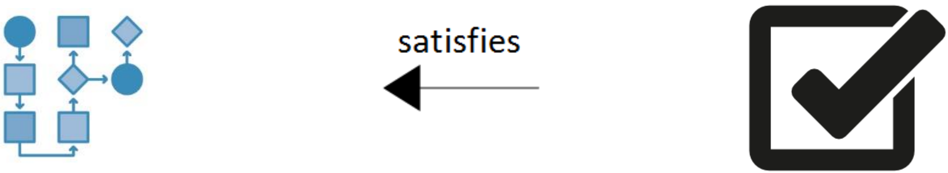
Formal Verification Techniques

– Design time
- E.g. Simulink Design Verifier
- Temporal logics / patterns
- Life sequence charts
- UML communication diagrams

– Run time
- Run time verification / monitoring
- Temporal logics

Motivation » Research Objectives





Specification Technique

– Abstract syntax

– Graphical notation

Rigorous Formalization

– Precise semantics

– Machine computable

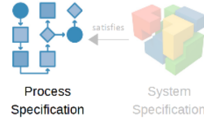
Verification Technique

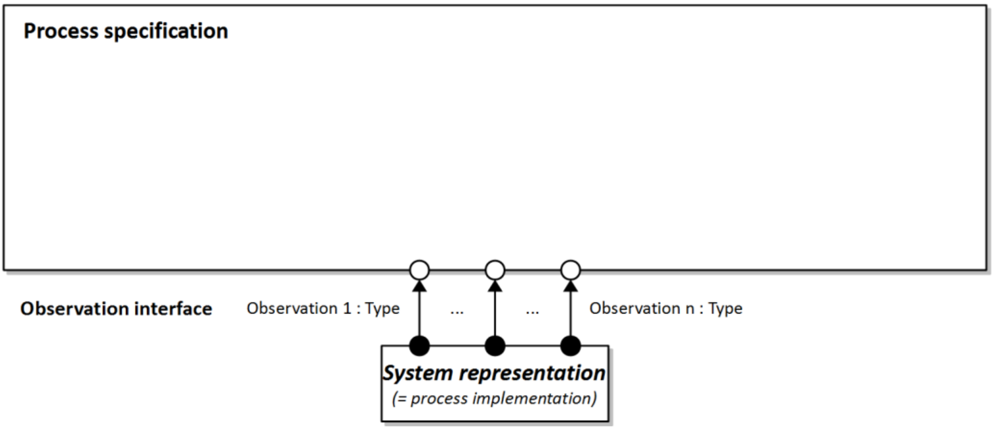
– Design time

– Run time

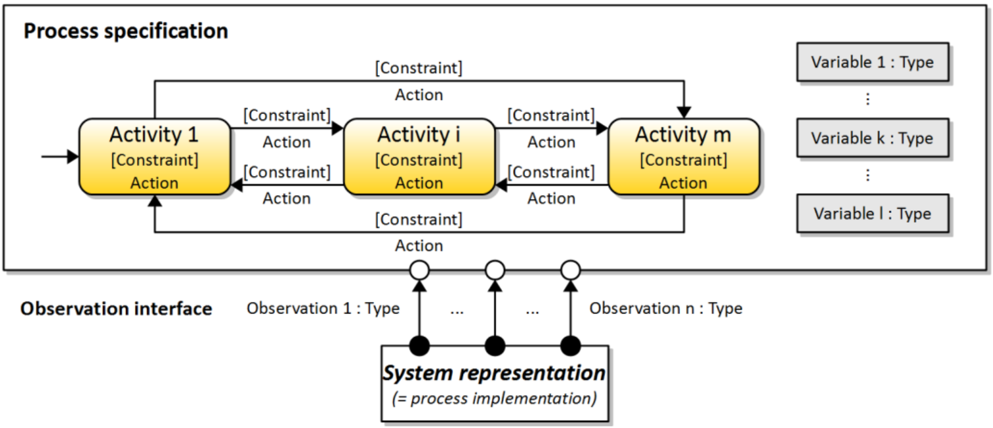
1. **Contribution**
2. Evaluation
3. Conclusion

Contribution » Specification Technique

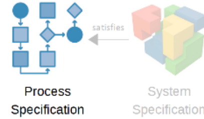


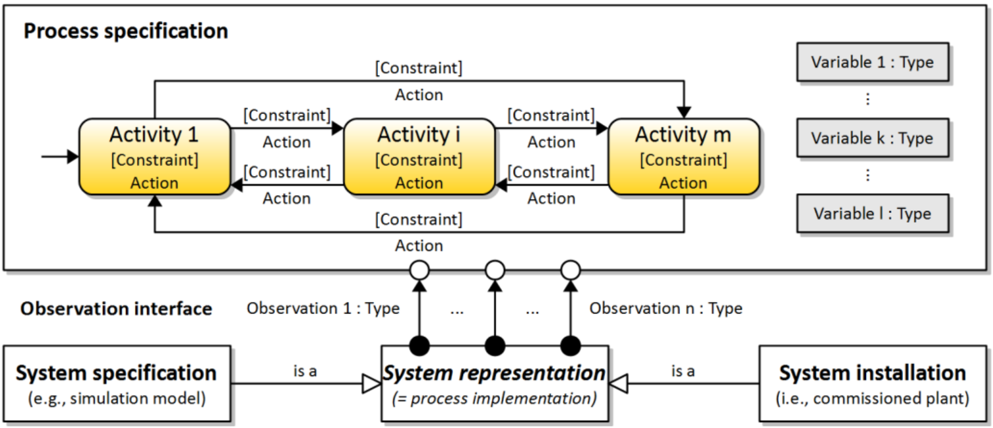


Contribution » Specification Technique

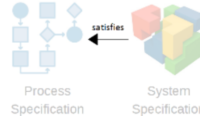


Contribution » Specification Technique





Contribution » Rigorous Formalization



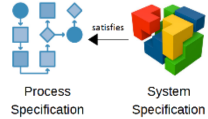
Definition 4 (Process satisfaction). *Given some process specification* $P = (A, M, N, O, V, T, a', v', f_1, f_2, g_1, g_2)$*, an observation trace* $\tau_n = (\omega_k)_{k=0}^{n}$ *and the respective process execution* $\pi_n = (\alpha_k, \omega_k, \phi_k, \beta_k)_{k=0}^{n}$*:*

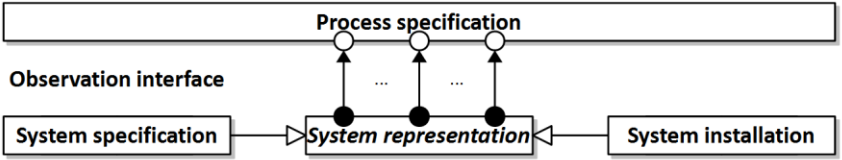
$$\tau_n \text{ satisfies } P \Leftrightarrow \forall k \in D : \beta_k = true$$

with $n \in \mathbb{N} \cup \{\infty\}$ *defining the sequence length and* D *representing the finite or infinite set of sequence indices:*

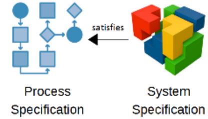
$$(n = \infty \Leftrightarrow D = \mathbb{N}) \wedge (n \neq \infty D = \{k \in \mathbb{N} : k \leq n\})$$

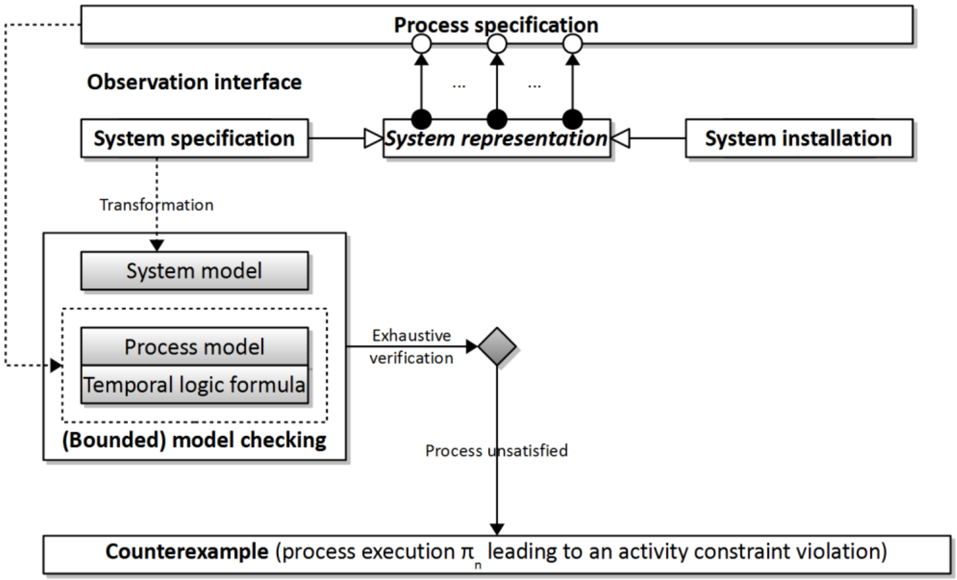
Contribution » Verification Technique



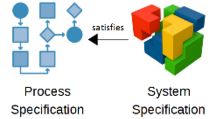


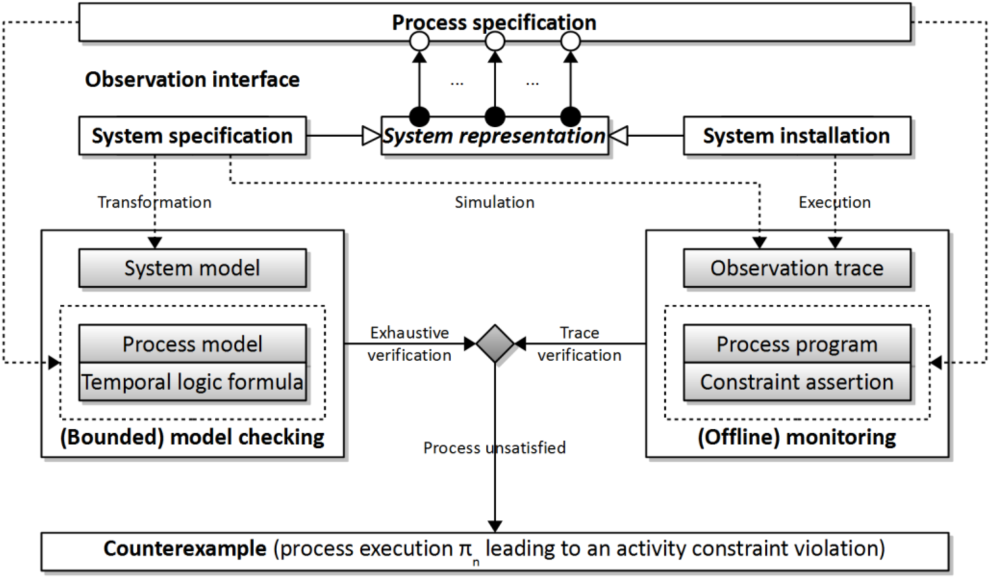
Contribution » Verification Technique





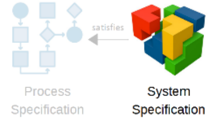
Contribution » Verification Technique



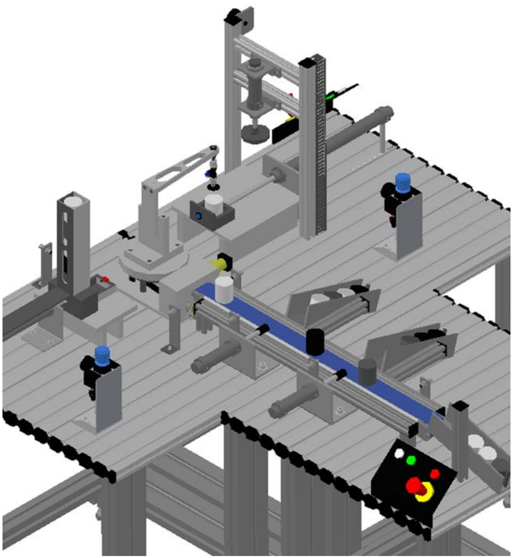


1. Contribution
2. **Evaluation**
3. Conclusion

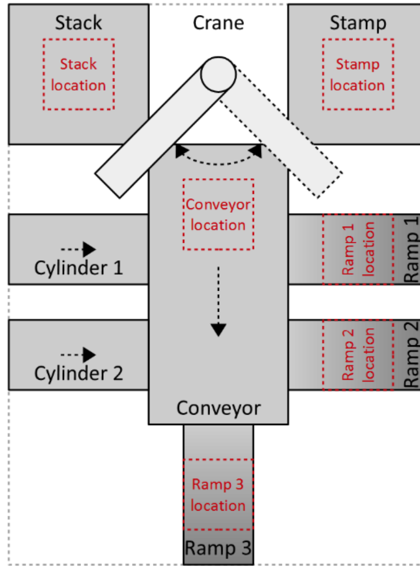
Evaluation » Pick and Place Unit



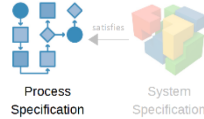
Geometric Setup

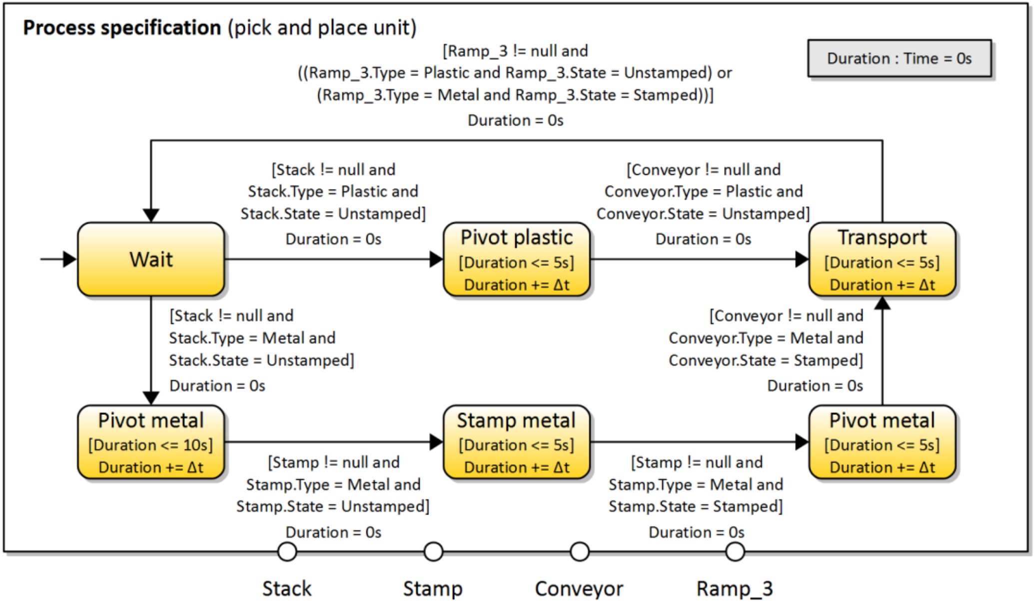


Plant Layout

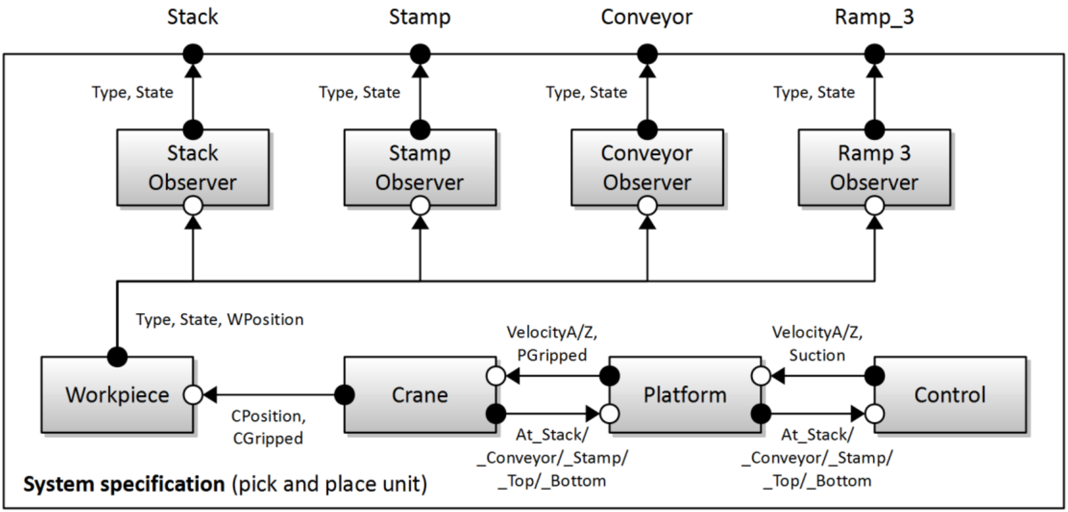


Evaluation » Process Specification

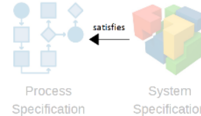




Evaluation » System Specification

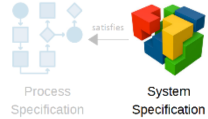


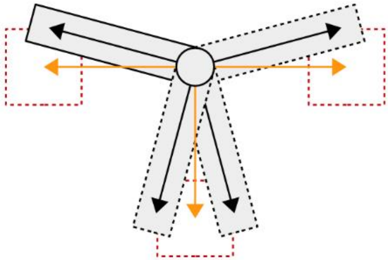
Evaluation » Satisfaction Verification

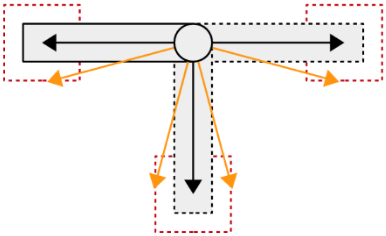


		Step	1	2	...	30	31	...	102	103
System model	Workpiece	WPosition	{A: 0, Z: 0}	{A: 0, Z: 0}	...	{A: 65, Z: 1}	{A: 70, Z: 1}	...	{A: 210, Z: 0}	{A: 210, Z: 0}
		...	...	...	...	...	...	...	...	...
	Crane	CPosition	{A: 0, Z: 0}	{A: 0, Z: 0}	...	{A: 65, Z: 1}	{A: 70, Z: 1}	...	{A: 210, Z: 0}	{A: 210, Z: 0}
		OSuction	false	false	...	true	true	...	false	false
		...	...	...	...	...	...	...	...	...
	...	...	...	...	...	...	...	...	...	...
Process model	Activity		Wait	Pivot metal	...	Pivot metal	Pivot metal	...	Pivot metal	Pivot metal
	Observations	Stack	{Type: Metal}	null	...	null	null	...	null	null
		...	...	...	...	...	...	...	...	...
	Variables	Duration	0.0s	0.1s	...	3.0s	3.1s	...	10.0s	10.1s
	Activity Constraint		true	true	...	true	true	...	true	false

Evaluation » Issue Analysis / Resolution







1. Initial System Specification

– Initial sensor positions

– Incorrect crane angles

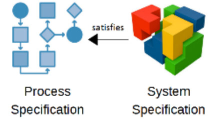
2. Revised System Specification

– Displaced sensor positions

– Correct crane angles

1. Contribution
2. Evaluation
3. **Conclusion**

Conclusion » Benefits and Future Work



Benefits

☑ Obervation interface allows to...

- Decouple and integrate process and system specification
- Model process specification over abstract observation streams
- Model system specification using observer components

☑ Verification technique allows to...

- Prove process satisfaction both at design and at run time

Future Work

☐ Improve graphical notation of the process specification

- Reduce modeling effort through inclusion of specification patterns

☐ Analyze and improve scalability of the presented approach

- Prove process satisfaction for the entire pick and place unit
- Prove process satisfaction step-wise from activity to activity?

Formal Technical Process Specification and Verification for Automated Production Systems

Georg Hackenberg, Alarico Campetelli, Christoph Legat,
Jakob Mund, Sabine Teufl and Birgit Vogel-Heuser