TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Institut für Computertechnik
Institute of Computer Technology

Consistency Verification of Processes: From Businesses to Cyber-physical Systems

Keynote

Hermann Kaindl

Based on
R. Hoch, C. Luckeneder, R. Popp and H. Kaindl, "Verification of Consistency between Process Models, Object Life Cycles, and Context-dependent Semantic Specifications," in *IEEE Transactions on Software Engineering*, doi: 10.1109/TSE.2021.3110191.

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

Introduction

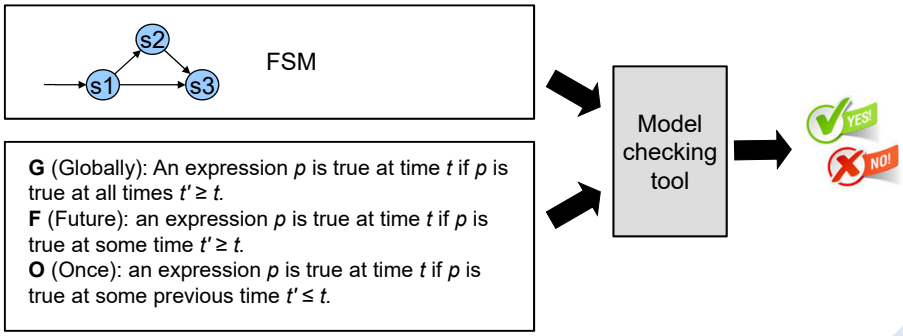
- Verification: building the system right
- Validation: building the right system
- Formal verification can provide certain guarantees.
- Business process model (BPM)
- Connection of control-flow models and object life cycles
- Semantic task / action specification (declarative)
- Formal verification of processes based on model checking
- Application to a cyber-physical (CPS) process — e-charging

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

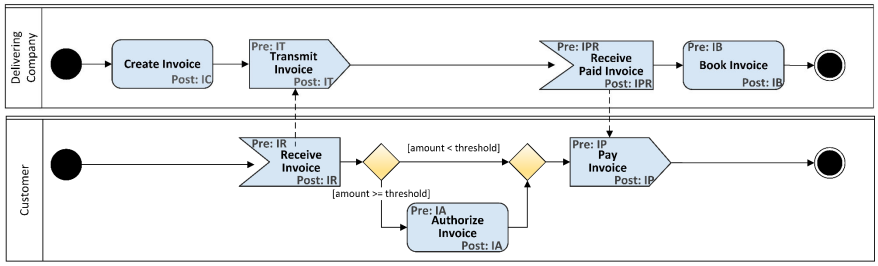
Background — Model Checking

- Model represented as *Finite State Machine* (FSM)
- Property formulas given in *Linear Temporal Logic* (LTL), more precisely PLTL (LTL with past).



Background — BPM as Activity Diagram

- Running example as an Activity Diagram (with annotations)

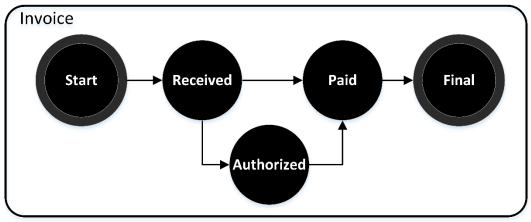


Post: IC = created(Invoice); Pre: IT = created(Invoice); Post: IT = transmitted(Invoice); Pre: IT = created(Invoice); Post: IT = transmitted(Invoice); Pre: IPR = transmitted(Invoice); Post: IPR = paymentReceived(Invoice); Pre: IB = paymentReceived(Invoice); Post: IB = booked(Invoice); Pre: IR = –; Post: IR = received(Invoice); Pre: IA = received(Invoice); Post: IA = authorized(Invoice); Pre: IP = received(Invoice); Post: IP = paid(Invoice);

- (Business) process model as control-flow (procedural)

Background — Object Life Cycle

- States (of an Invoice object) and transitions among them



- Transition conditions still to be defined here

Background — Semantic Action Specification

- Cf. semantic specification of (Web) services
- Pre- and postconditions

Receive Invoice:
Pre: —
Post: received(Invoice)

- Declarative representation

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

V&V Mismatch — No problem first

- Formal verification of composed action against the specifications of its atomic actions

$< Receive\ Invoice,\ Pay\ Invoice >$

Sequence <Receive Invoice, Pay Invoice>:
Pre: —
Post: paid(Invoice)

Pay Invoice:
Pre: received(Invoice)
Post: paid(Invoice)

- Verification and validation (V&V) straight-forward
- In a "larger" (hypothetical) company, an additional action for authorization:

Authorize Invoice:
Pre: received(Invoice)
Post: authorized(Invoice)

V&V Mismatch — The Problem

- Business process with additional authorization:

  $< Receive\ Invoice,\ Authorize\ Invoice,\ Pay\ Invoice >$

- Formal verification succeeds again.
- This is also a valid business process.
- Verification also succeeds for

  $< Receive\ Invoice,\ Pay\ Invoice,\ Authorize\ Invoice >$

- but not validation!
- Same for many other processes including authorization in the action composition

V&V Mismatch — Extending the semantic action specification

- Additional precondition (about the invoice being authorized)
- Avoids the successful verification of these invalid processes
- Original process *cannot* be verified anymore!

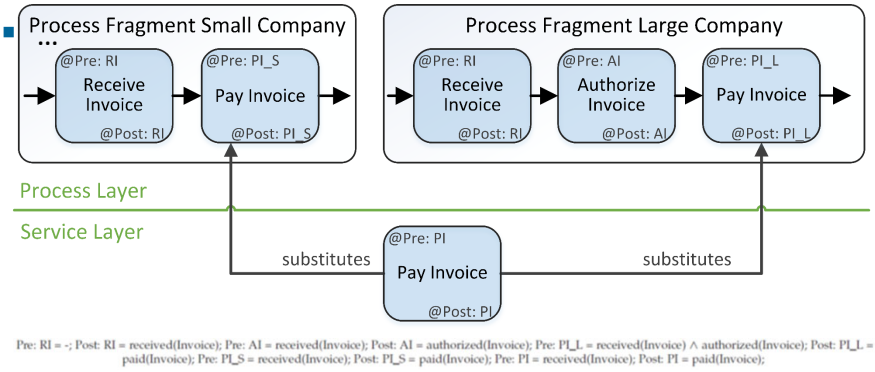
  $< Receive\ Invoice,\ Pay\ Invoice >$

- Mismatch of semantic specification and implementation, more precisely an overspecification
- Additional knowledge encoded not directly related to these implementations per se

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

Context-dependent Semantic Action Specification



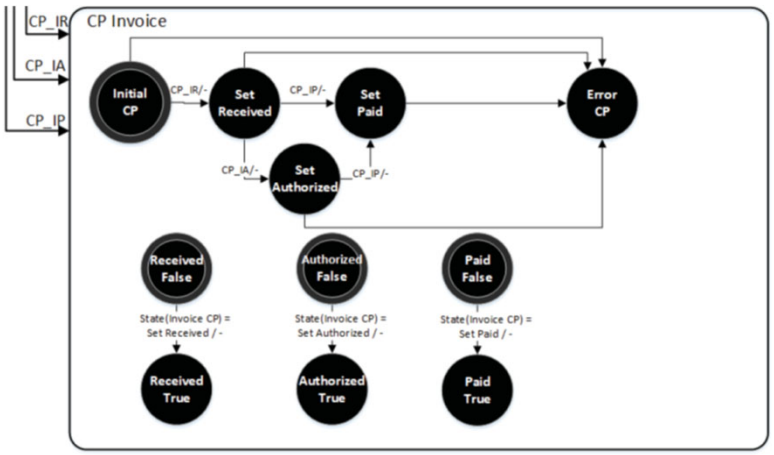
- The *Pay Invoice* action in the context of the large company has an additional precondition, *authorized(Invoice)*.
- The subtype relationship guarantees substitutability.

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

Extended Object Life Cycles — Attributes

- Extending with attributes for memorizing previous states



Extended Object Life Cycles — CPS

- Both software and physical parts
- Possible interaction between physical objects solely based on some physical law
- A physical property of one object modeled as an attribute in its extended life cycle
- Can be changed from a life cycle model of another physical object
- May lead to asynchronous communication between the extended object life cycles that model physical objects
- Another way of communication in addition to the software communication

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

Grounding of Action Specifications in Life Cycles

- To define the real meaning of the semantic action specifications in the process models
- Predicates formulated in terms of the attributes
- Pay Invoice Action formalized using grounded predicates:

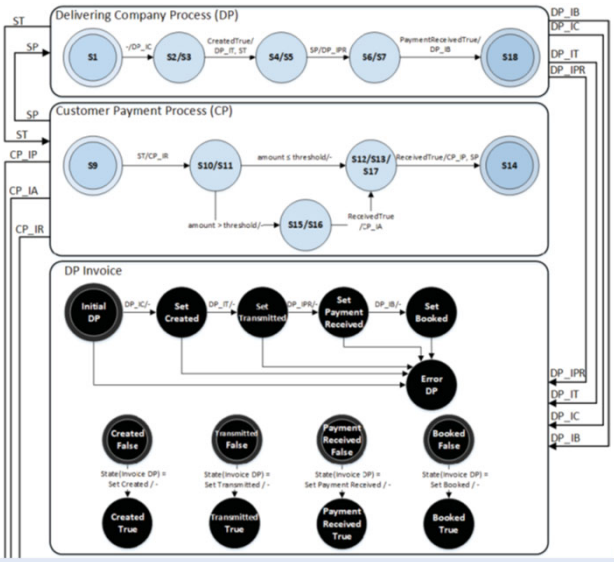
Pay Invoice:
Pre: attributeIsSet(InvoiceCPReceived, ReceivedTrue)
Post: attributeIsSet(InvoiceCPPaid, PaidTrue)

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

Verification Through Model Checking — FSMs

- Model-checker tool nuXmv
- Verification of consistency



Verification Through Model Checking — Consistency

- Consistency verification
- All the involved specifications 'fit together', both procedurally and logically.
- The process model (or a defined part of it) can continue with an action based on the given state of the object life cycle: *F*(*DefStates*), and
- The object life cycle can handle a given action in a given state: *G*(¬*Error*)
- nuXmv takes a few seconds on a laptop computer for verifying this running example.

Verification Through Model Checking — Context-dependent Semantic Specifications

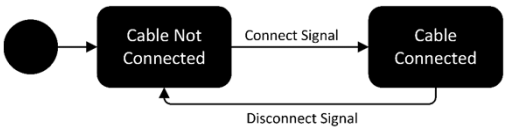
- The role of context-dependent semantic specifications for verification
- They constrain the possible transitions in the models, which makes the verification stricter.

Agenda

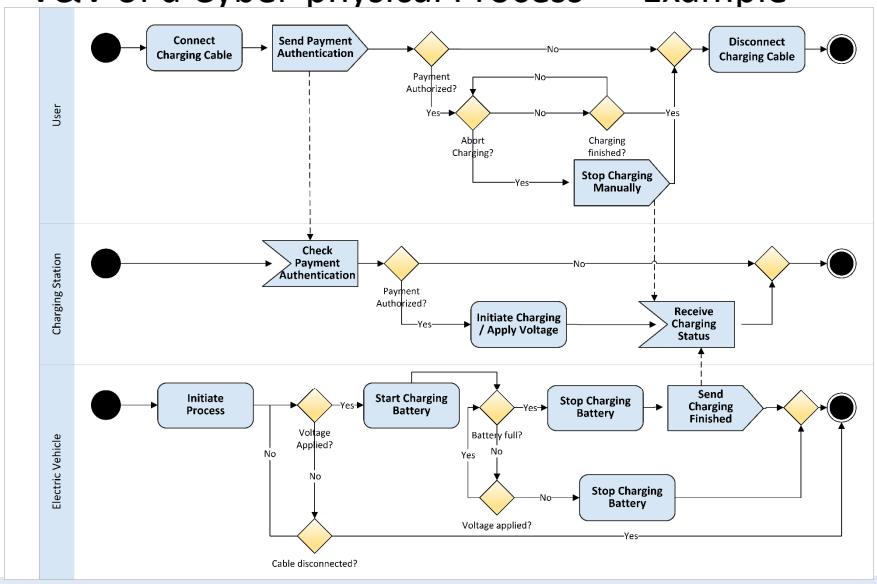
- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

V&V of a Cyber-physical Process

- Case study of a real-world cyber-physical process for charging an electric vehicle at a charging station
- Several iterations of verification and validation
- Physical interaction in CPS:
  establishing a physical connection via cable between two physical devices
- Non-monotonicity



V&V of a Cyber-physical Process — Example



V&V of a Cyber-physical Process — Lessons Learned

- Automated consistency verification of such a process helps finding related problems in the models, of course.
- Complementary to validation of the process, which requires knowledge of domain experts and their precious time
- Even skilled modelers are struggling to create formally correct processes.
- The interpretation of the counterexamples as listed by the nuXmv tool is difficult, as they are very verbose.
- The successful verification run (for checking our two consistency properties) on the final model took about 11 seconds on a laptop computer.

Agenda

- Introduction
- Background
- V&V Mismatch
- Context-dependent Action Specifications
- Extended Object Life Cycles
- Grounding of Action Specifications in Life Cycles
- Verification Through Model Checking
- V&V of a Cyber-physical Process
- Conclusion

Conclusion

- New major contributions:
- Grounding of semantic action specifications in (extended) object life cycles
- Extending object life cycles with attributes
- Supporting processes including non-monotonicity
- Modeling communication based on physical interaction in cyber-physical systems
- Our integration of procedural and declarative specifications facilitates a comprehensive verification approach for consistency.

Acknowledgments

- Most of this work has been performed together with project members, most notably the co-authors of the IEEE TSE paper Ralph Hoch, Christoph Luckeneder, and Roman Popp.
- Part of this research has been carried out in the ProREUSE project (No. 834167), funded by the Austrian FFG, FeatureOpt project (No. 849928), funded by the Austrian BMVIT (represented by the Austrian FFG) and the VerASoS project (No. 861210), funded by the Austrian FFG.
- We thank our industry partners, especially Christian Zeidler and Roland Kuras.