Automated Analysis of Industrial Workflow-based Models

Mario Cortes-Cornax
Adrian Mos
Ajay Krishna
Gwen Salaün

The 33rd ACM/SIGAPP Symposium On Applied Computing
Pau, France
10 April, 2018

Talk Overview

I. Introduction to Mangrove

II. Verification framework

III. Behavioural verification

IV. Data-based analysis

V. Case study

Mangrove

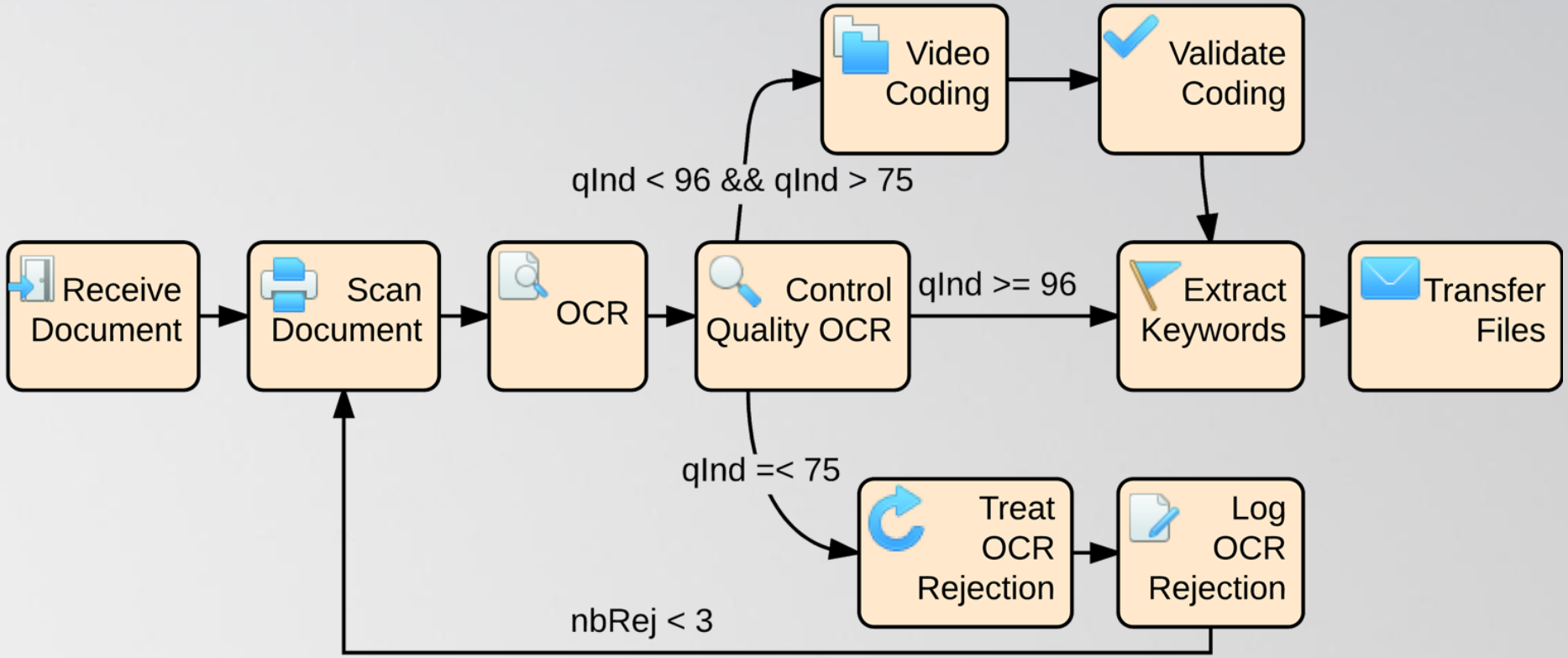
Domain specific process modelling language

Domain-dependent and platform independent

Unifies Business process and SOA

Establishes concept mappings between domain specific concepts and process activities

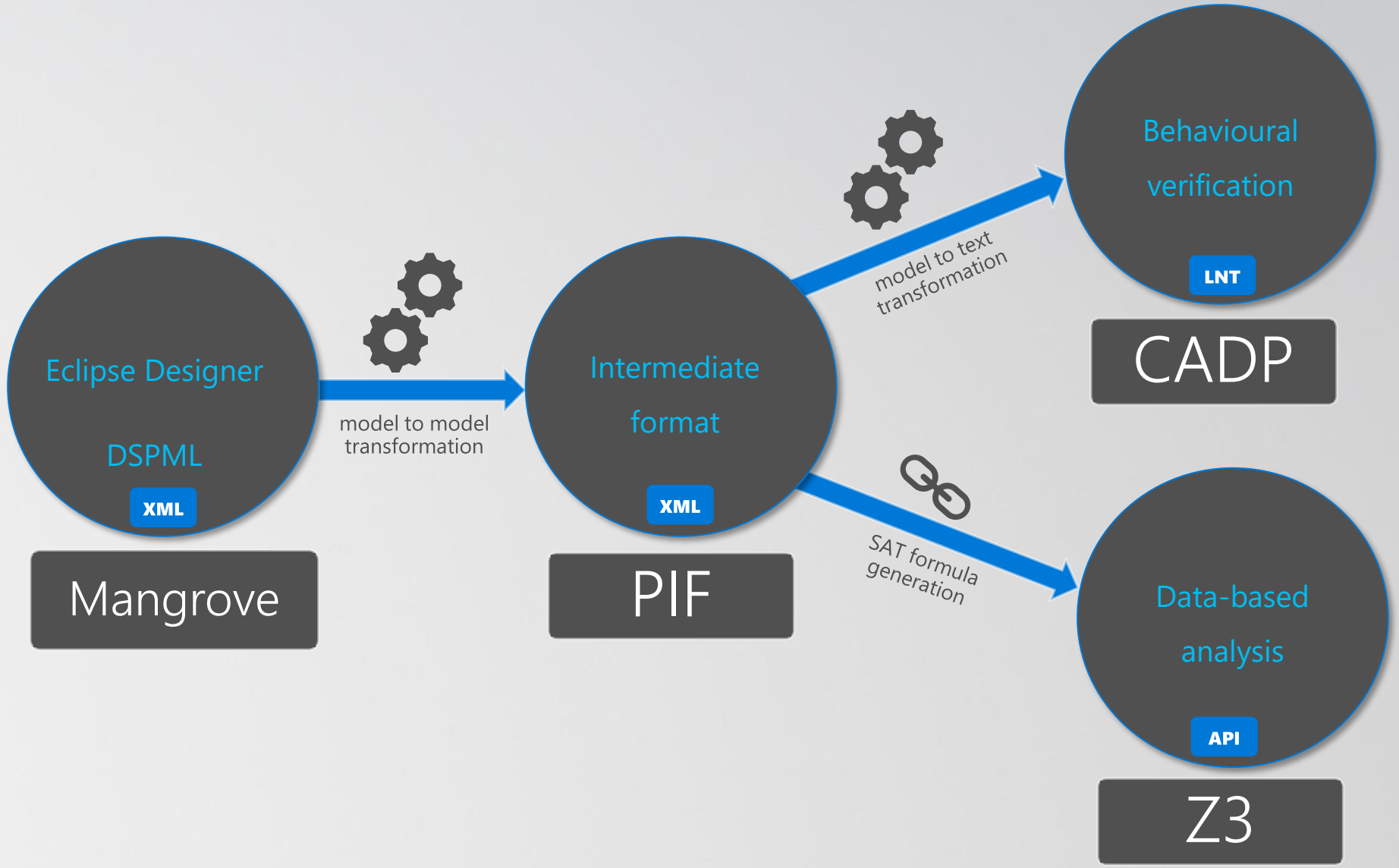
Mangrove Elements: Publishing System



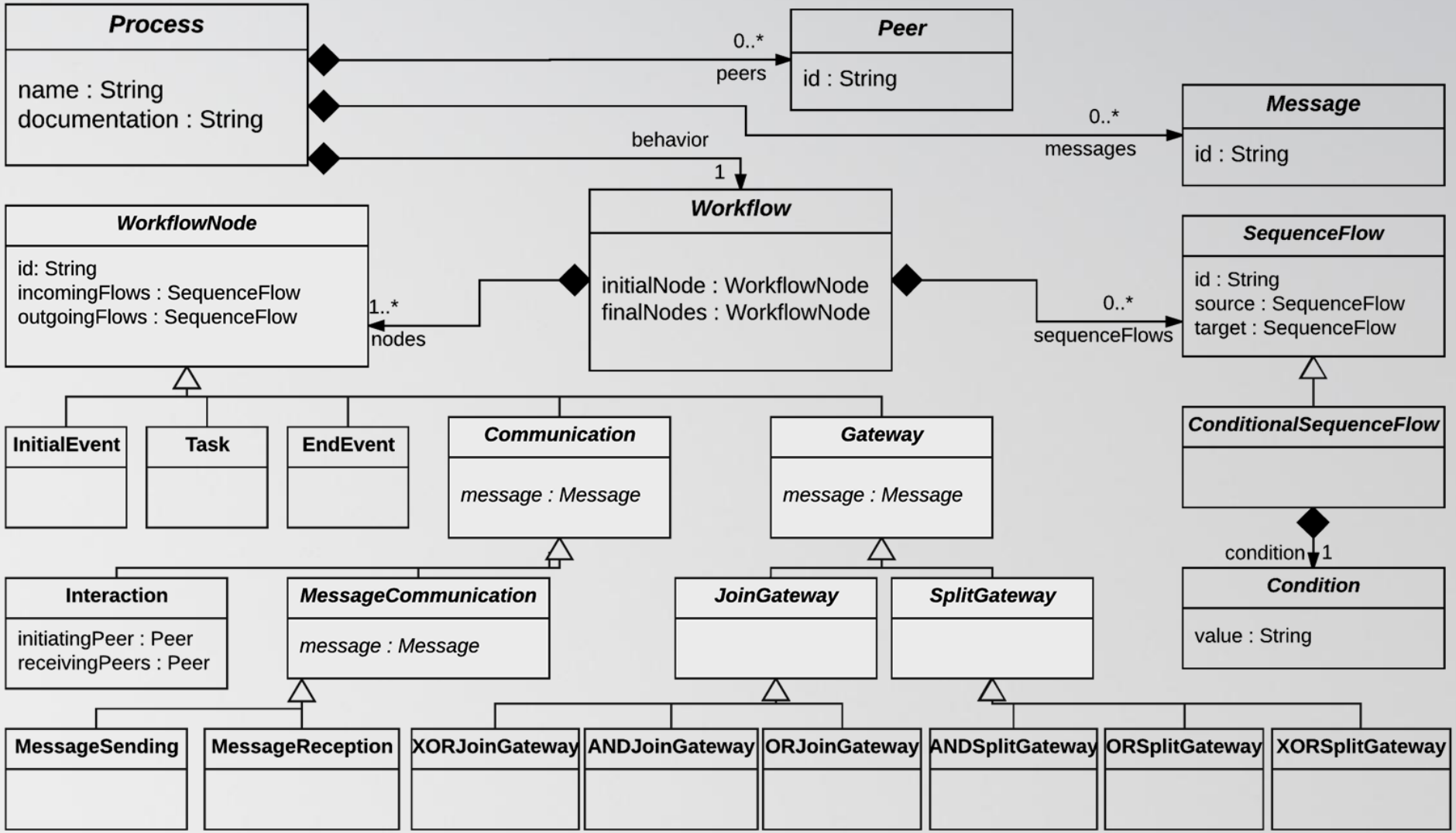
Step

Conditional Flow

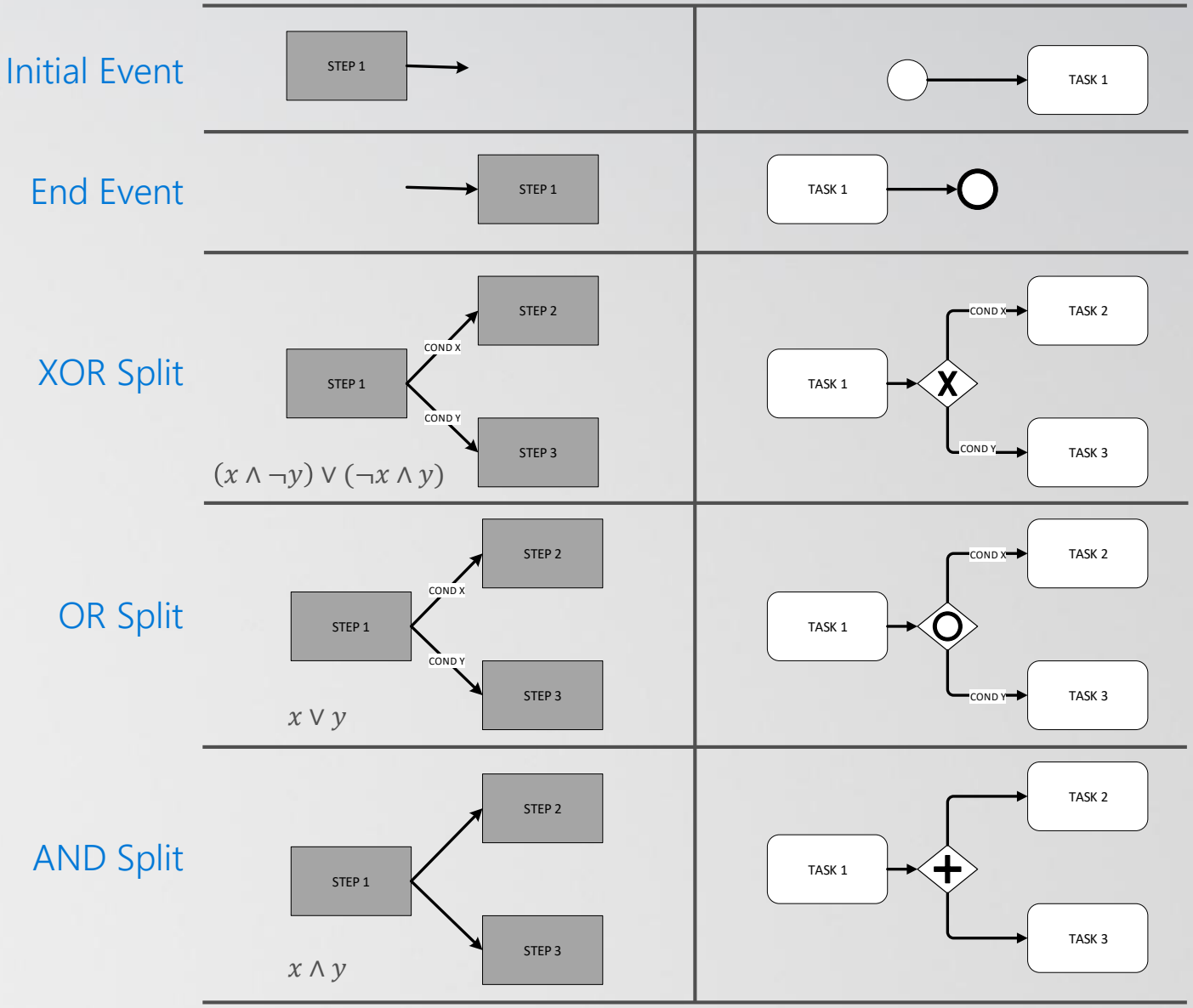
Automated Verification



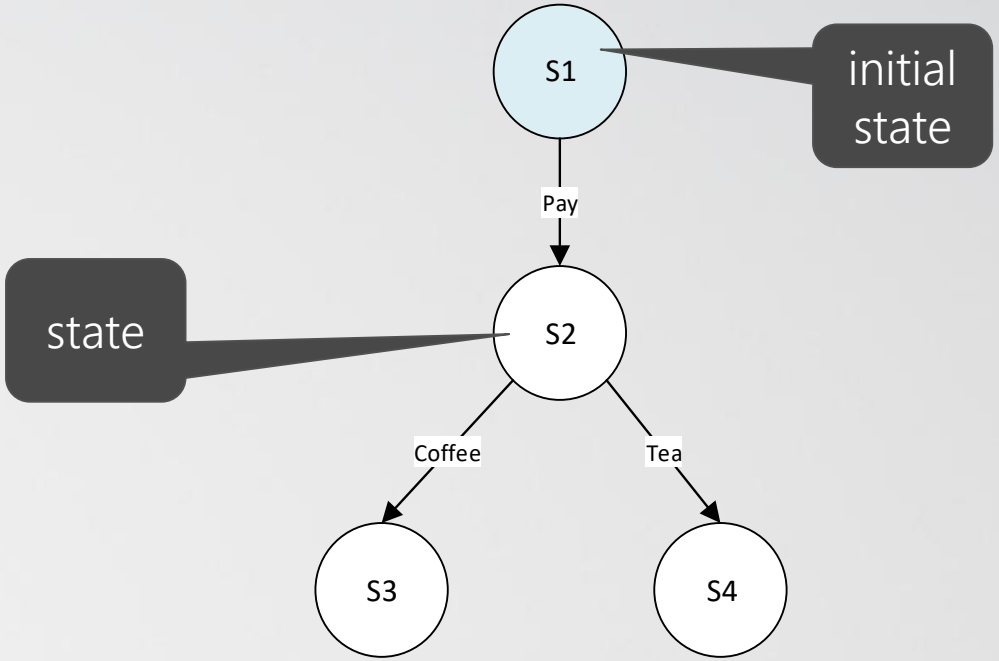
Process Intermediate Format (PIF)



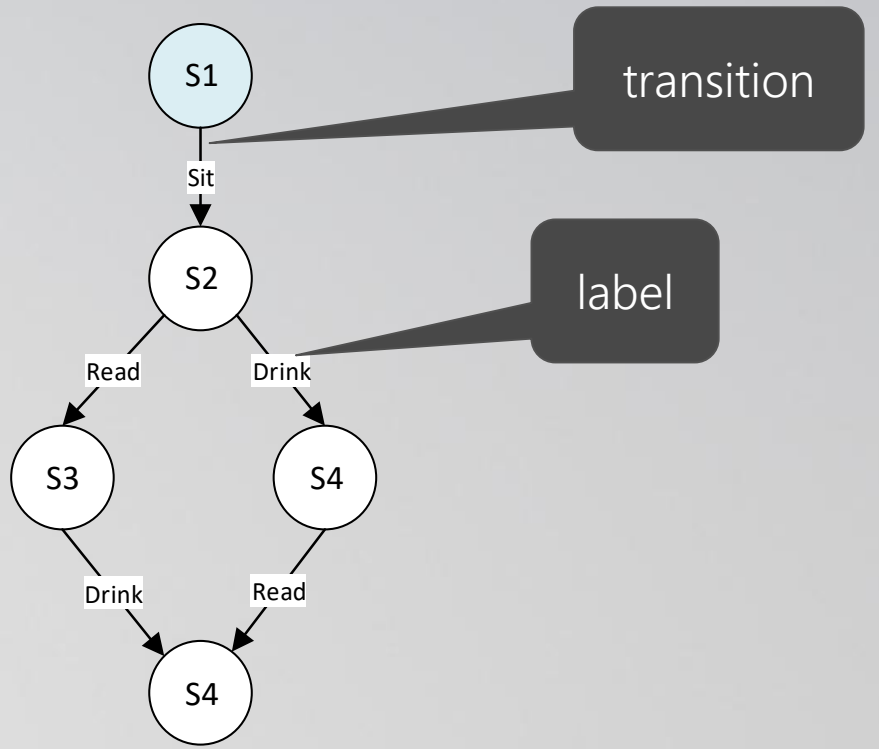
Mangrove to PIF Transformation



Labelled Transition Systems (LTS)



Choice



Interleaving

Semantic model for LNT

Functional Verification

Deadlock Freedom

not < true* > [true] false

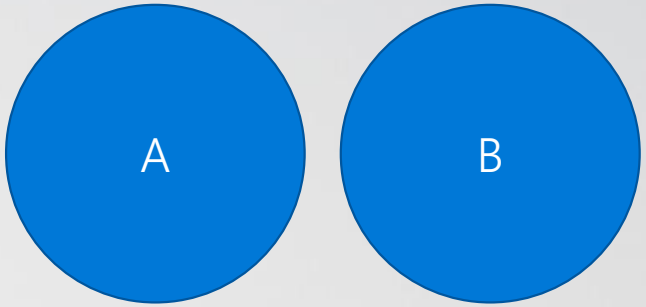
Safety Properties

[true* . REQ0 .(not REL0)* . REQ1] false

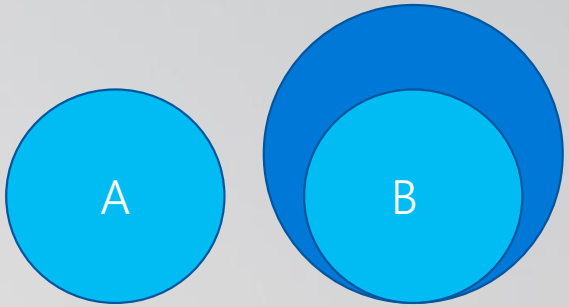
Reachability

< true*. PUT .true* . GET > true

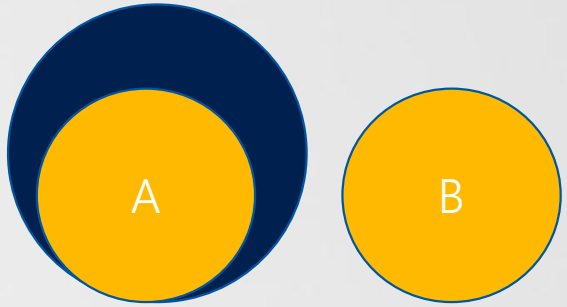
Process Comparison



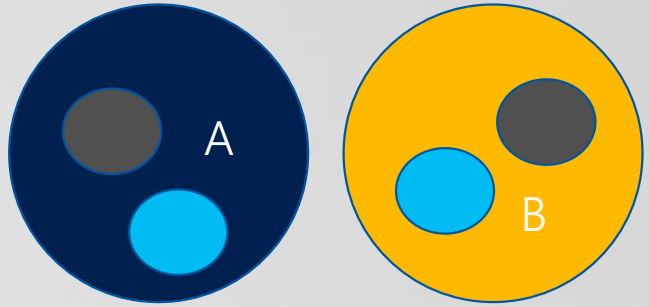
Conservative



Inclusive



Exclusive



Selective

Equivalence checking using CADP toolset

Data in Mangrove

- Data is not considered until now
- Behavioural model is an over approximation
- Possible “false-negatives” in verification

Modelling Mangrove Data

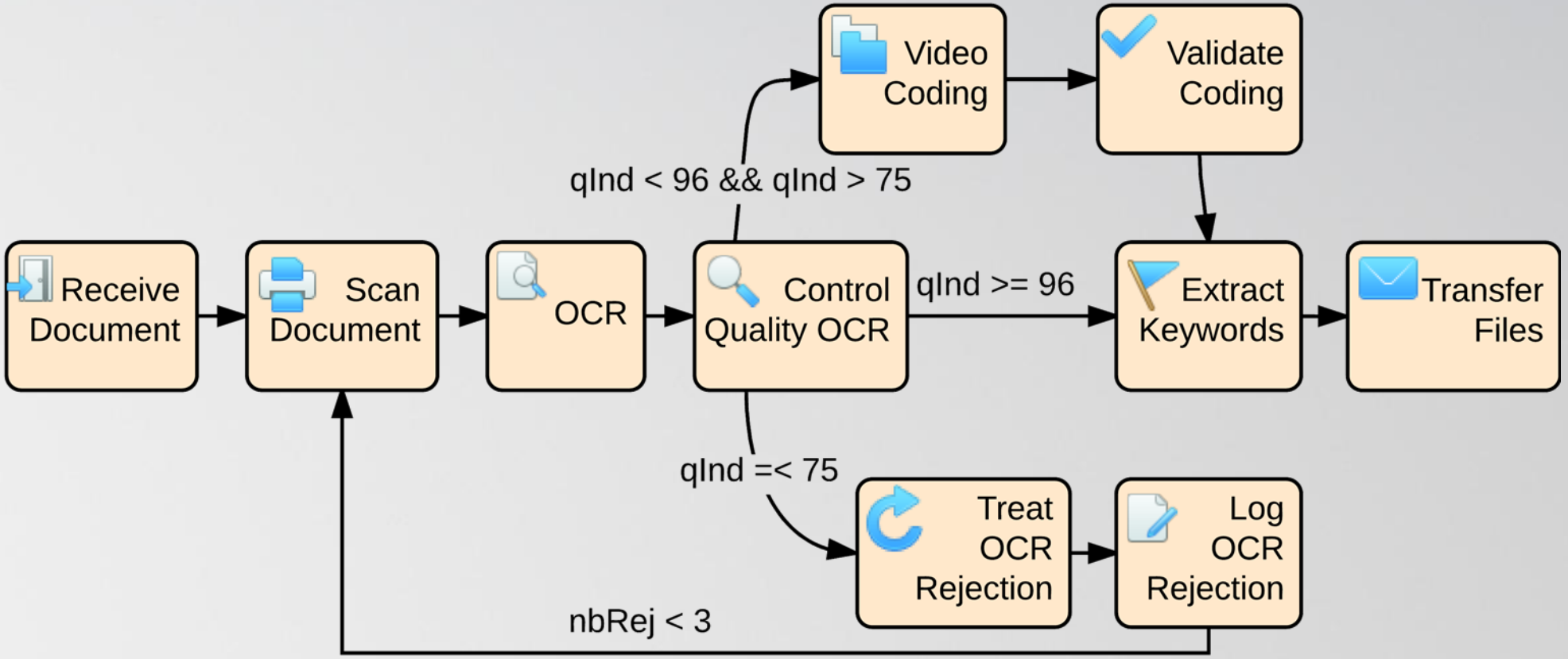
- Mangrove flows are directed by conditions
- Conditions can be modelled as satisfiability (SAT) constraints
- SAT constraints can be fed to a SAT solver to detect infeasible paths

$$((exp \geq 125 \wedge exp \leq 678) \wedge (age \geq 45 \wedge age \leq 90) \wedge (exp \geq 100) \wedge (age = 30))$$

Behaviour Refinement using SAT

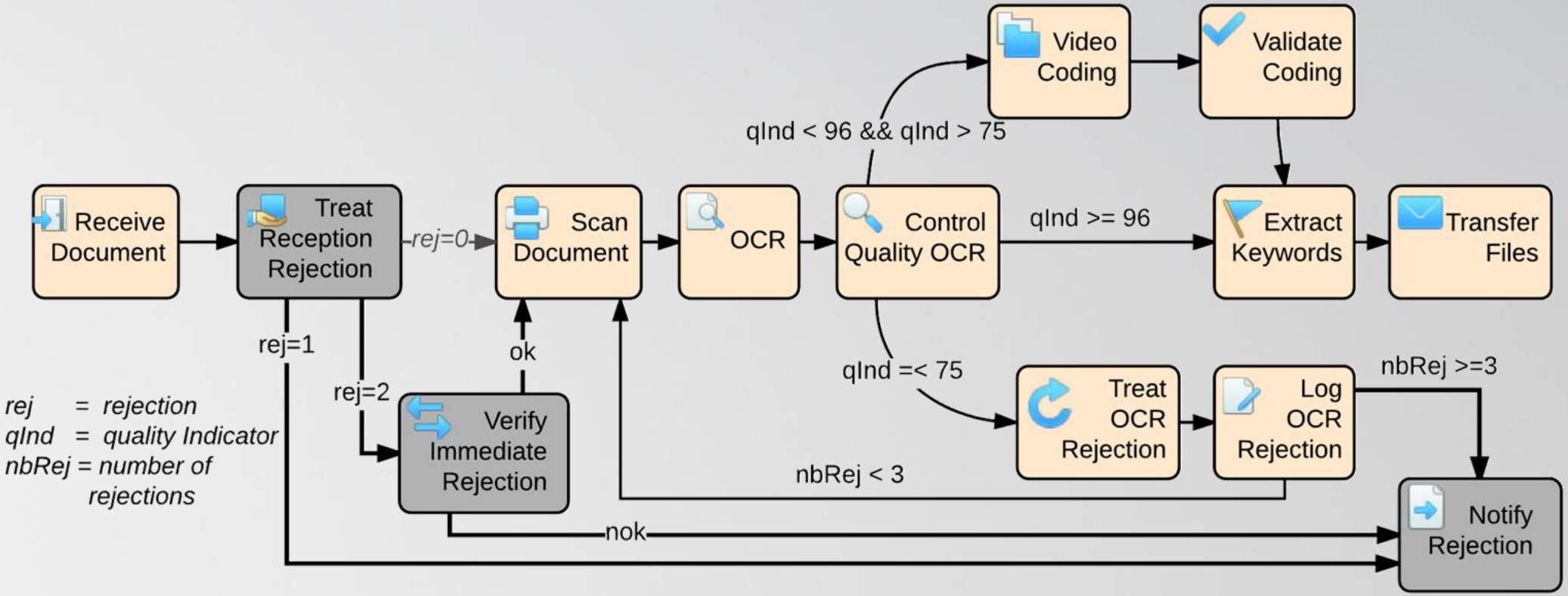
XML | Java | Z3 SMT Solver | Java | Java StaX | CADP

Document Processing



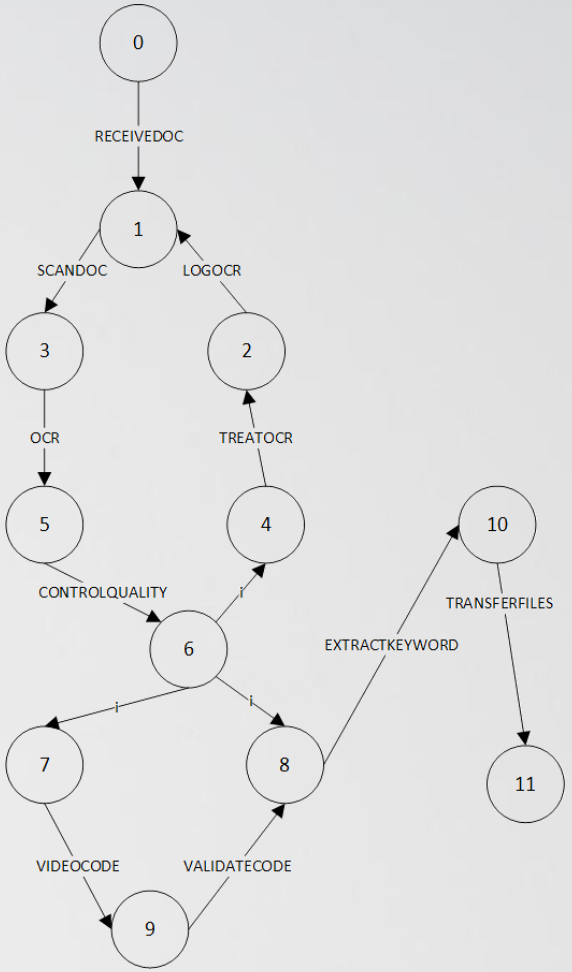
Model #1

Document Processing

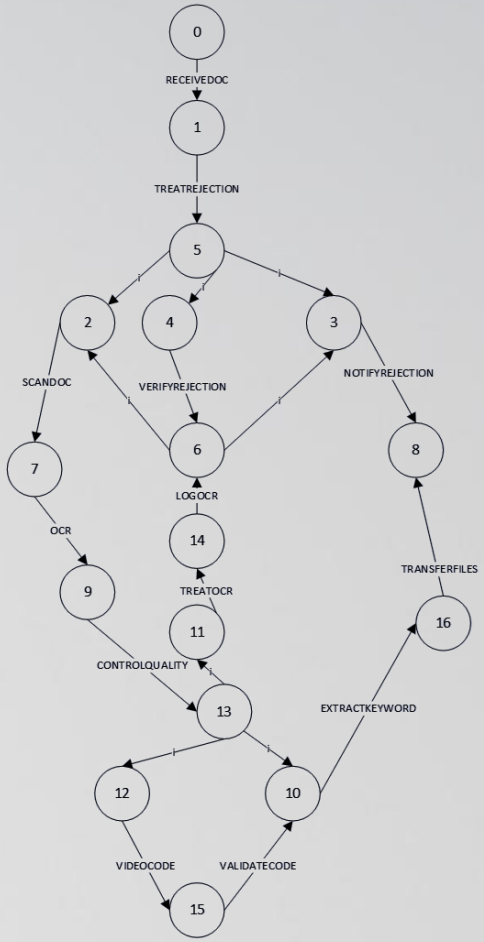


Model #2

Labelled Transition Systems



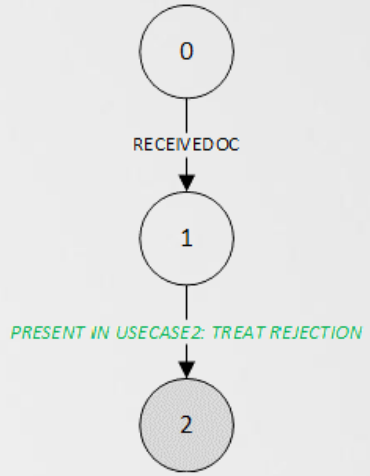
Model #1



Model #2

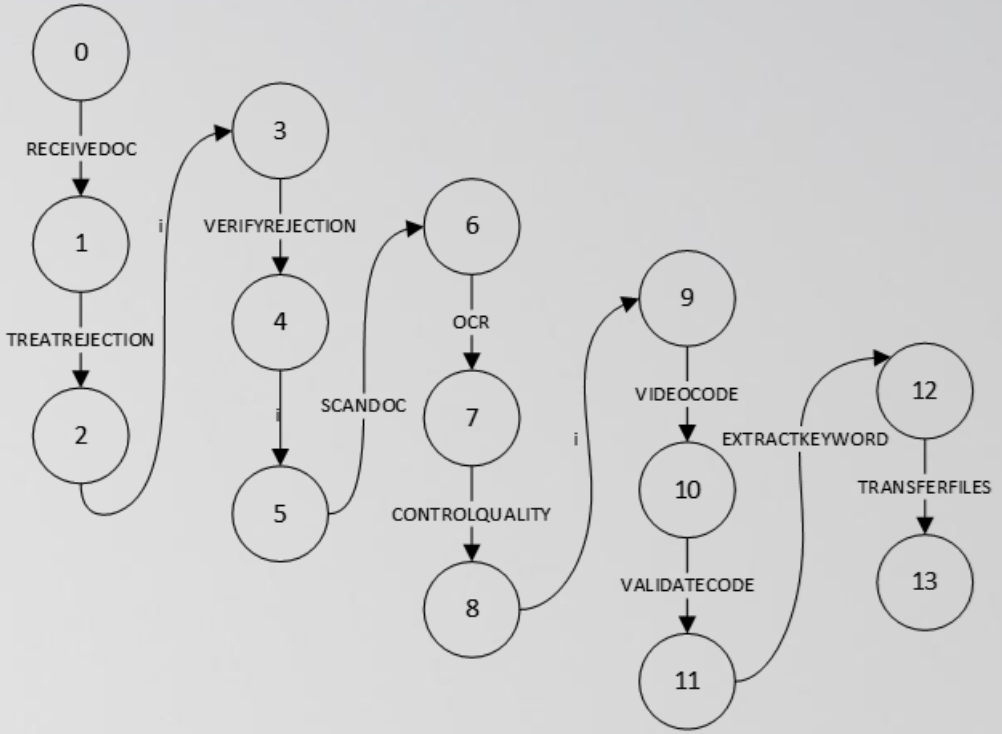
Behavioural Verification

- Do the processes evolve conservatively?



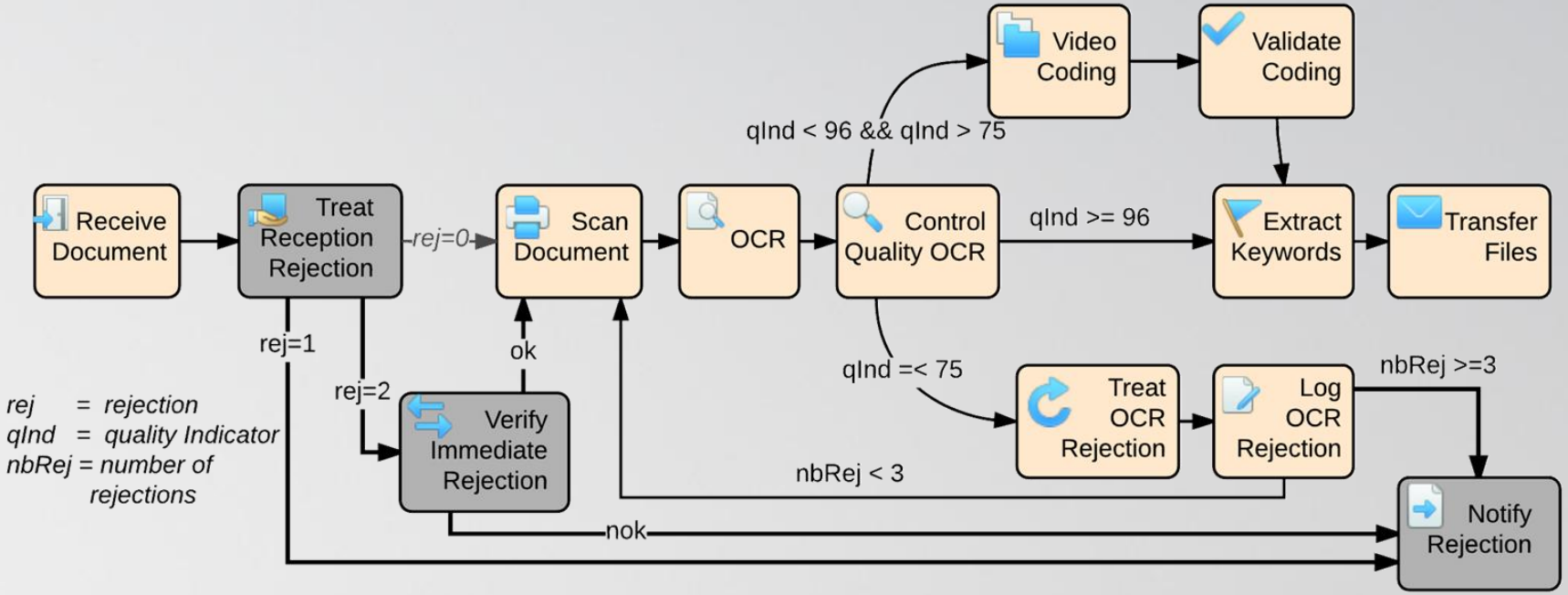
No

- Whether all rejections are notified in Model #2 ?



No

Data-based Analysis



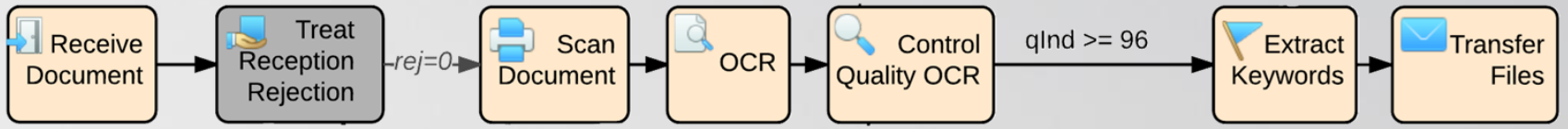
Assume, dataset is high quality i.e. qInd ≥ 96

$$((rej = 0 \oplus rej = 1 \oplus rej = 2) \Lambda (qInd \leq 75))$$ UNSAT

$$((rej = 0 \oplus rej = 1 \oplus rej = 2) \wedge (qInd > 75 \ \wedge qInd < 96))$$ UNSAT

$$((rej = 0 \oplus rej = 2) \Lambda (qInd \geq 96))$$ SAT

Data-based Analysis



Assume, dataset is high quality i.e. qInd ≥ 96

$$((rej = 0 \oplus rej = 1 \oplus rej = 2) \wedge (qInd \leq 75))$$ UNSAT

$$((rej = 0 \oplus rej = 1 \oplus rej = 2) \wedge (qInd > 75 \wedge qInd < 96))$$ UNSAT

$$((rej = 0 \oplus rej = 1 \oplus rej = 2) \wedge (qInd \geq 96))$$ SAT

Concluding Remarks

Behavioural Analysis

- Identifies erroneous behavior
- Checks correctness of model evolution

Data-based Analysis

- Refines the model
- Identifies infeasible paths

Future Work

Non-functional properties:

- Execution time
- Optimal resource allocation

Thank you!

ajaykrishna