Automatic Calculation of Coverage Profiles for Coverage-based Testing

Raimund Kirner, Walter Haas
Vienna University of Technology, Austria

Real-Time Systems Group

funded by the FWF project SECCO

Structural Code Coverage Metrics to Guide Software Testing

- Path Coverage:
  each path of the CFG is tested (infeasible in practice)
- State Coverage:
  each reachable state (variable values + program counter + HW states) is tested → most complex metrics (infeasible in practice)
- Statement Coverage:
  each statement is executed at least once
- Decision Coverage (aka. Branch Coverage):
  each edge of the CFG is executed at least once → tests conditional branches for both outcomes

Terminology

test data (TD)

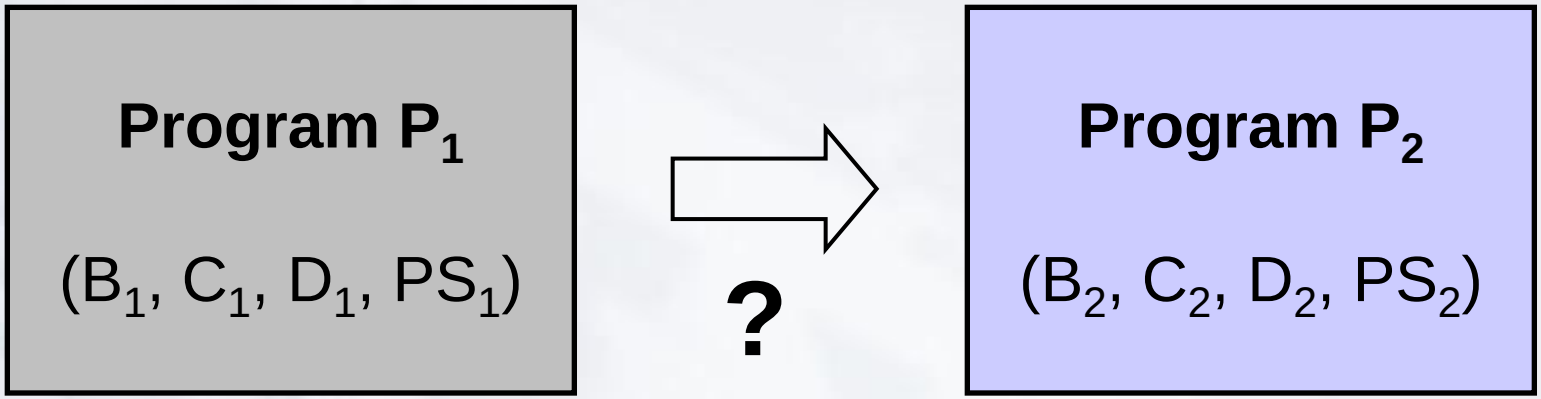
input data (ID)

```
task 1 (int a, long v) {
   …
   if (a<0 && v>0)
      v=0;
}
```

decision (D)

conditions (C)

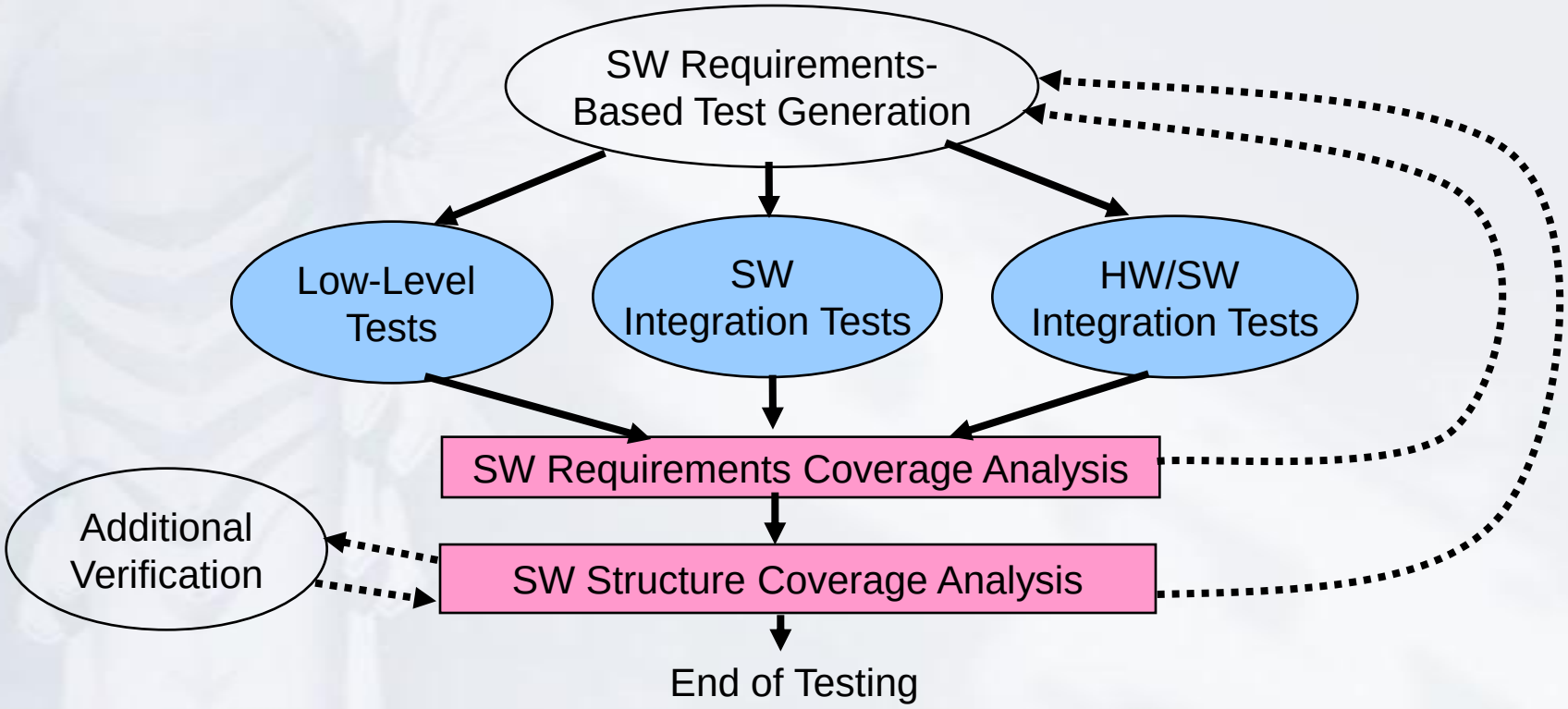
Question: Are Coverage Metrics Preserved by Code Transformations?



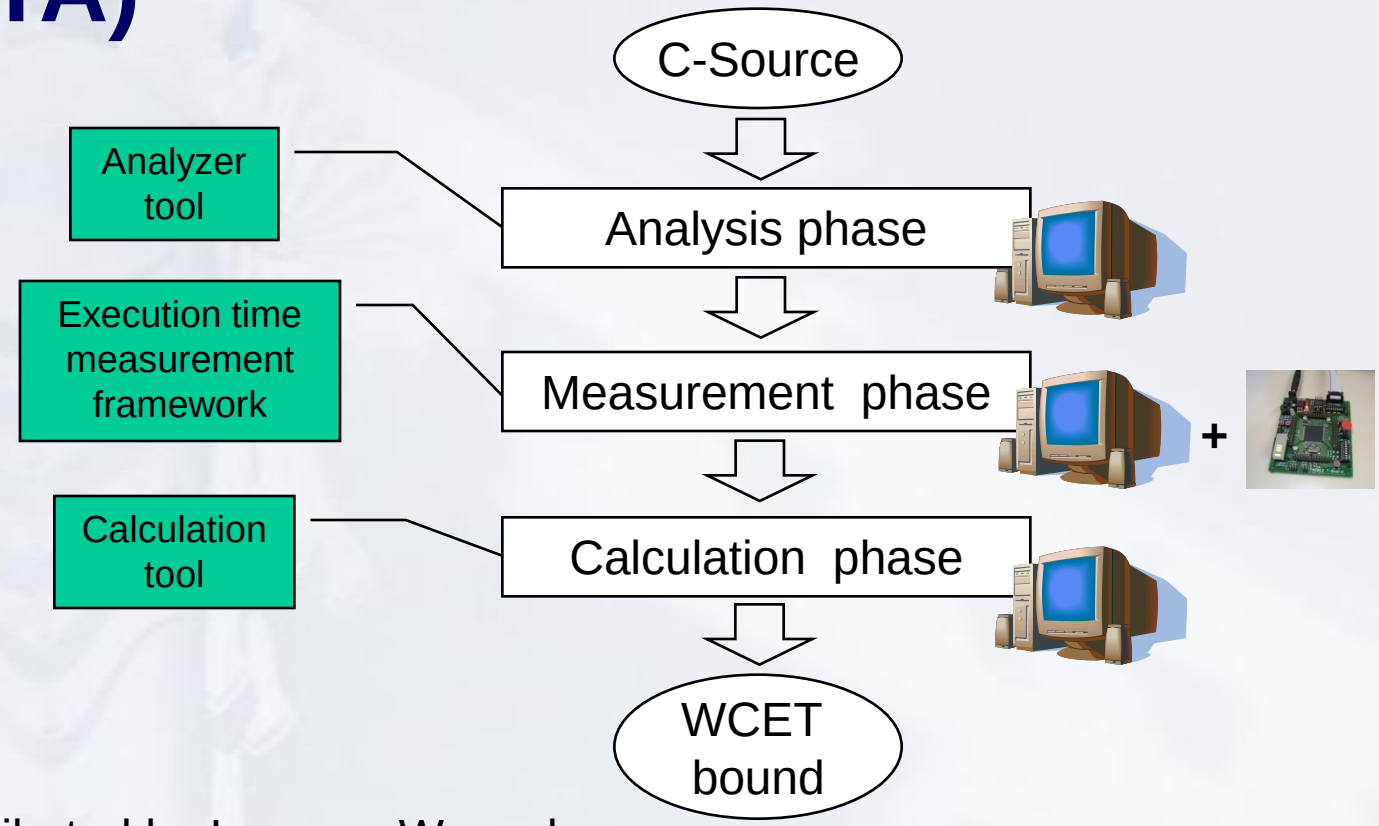
coverage(P_1, TD) $\equiv$ **coverage(P_2, TD)**

RTCA/DO-178b (Civil Avionics)

- Software testing process according to DO-178b:

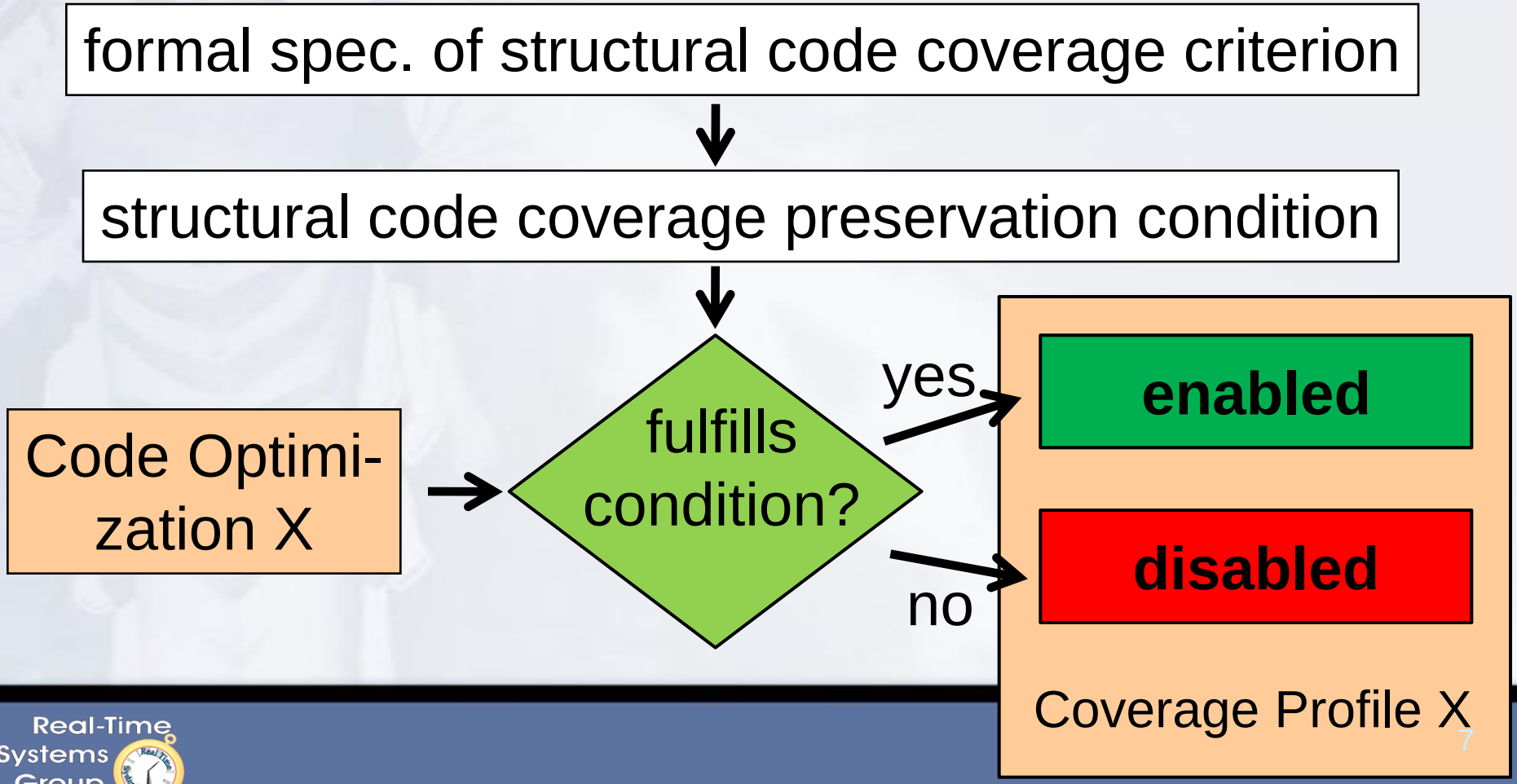


Measurement-based Timing Analysis (MBTA)

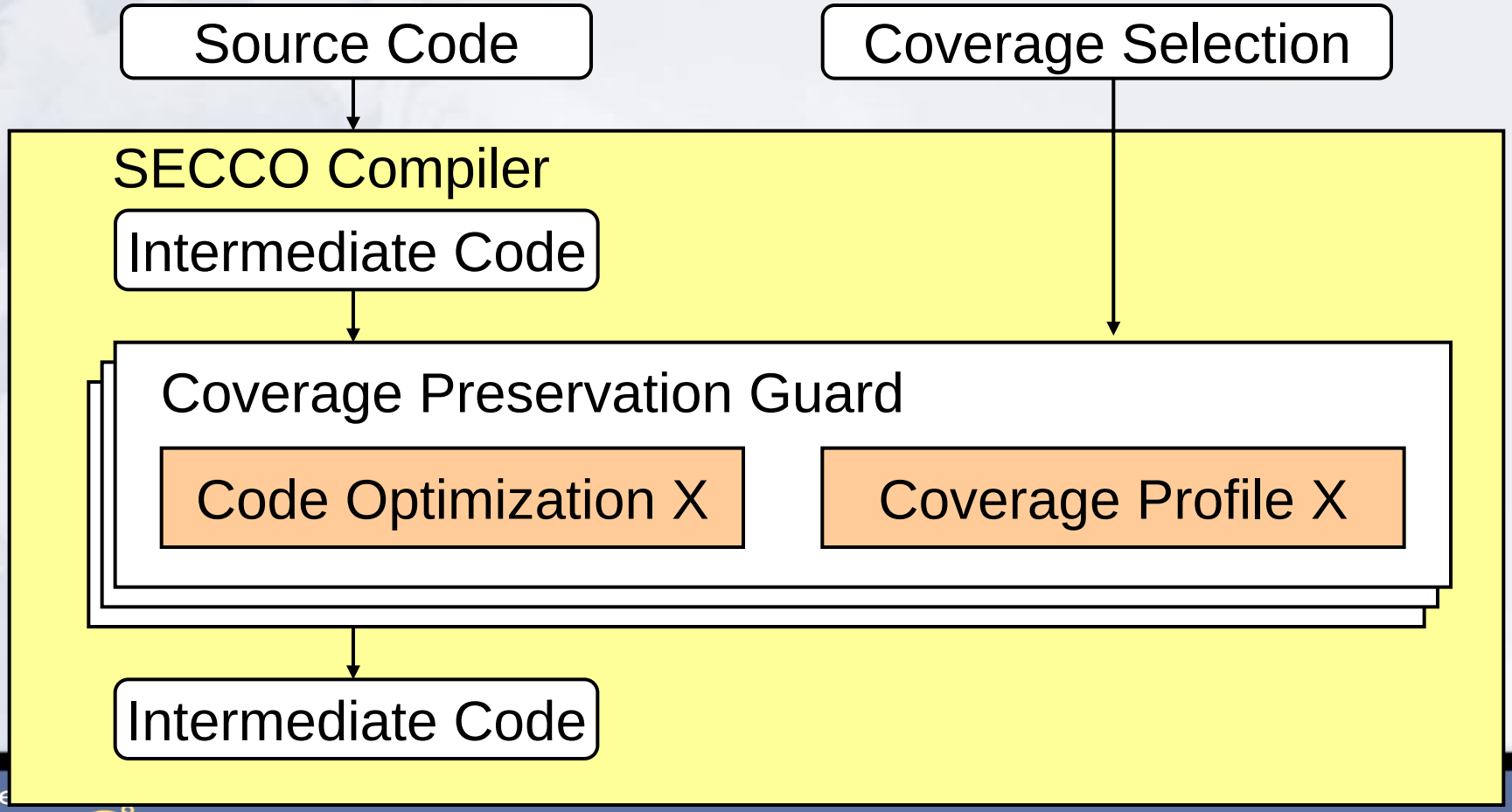


slide contributed by Ingomar Wenzel

The SCCP/x Coverage Profiles



The SCCP/x Compilation Profile



Formal Notations

- **Reachability Valuation:** $\mathbf{IV_R(x)}$
  … set of valuations of input variables that trigger the execution of expression X.

- **Reachability Valuation:** $\mathbf{IV_T(x)}$, $\mathbf{IV_F(x)}$
  … set of valuations of input variables that trigger the execution of boolean expression X with a certain result of X:
  $IV_T(x)$ … x evaluates to TRUE
  $IV_F(x)$ … x evaluates to FALSE

Preservation of Decision Coverage

- **Formal Definition of DC:**

  $\forall d \in D . (IV_T(d) \cap TD) \neq \phi \ \wedge (IV_F(d) \cap TD) \neq \phi$

  D … set of decisions in the program

- **DC Preservation Condition:**

  $\forall d_2 \in D_2 \ \ \exists d_1 \in D_1 . \text{touches\_ID}(d_1, IV_T(d_2)) \ \wedge$

  $\exists d_1 \in D_1 . \text{touches\_ID}(d_1, IV_F(d_2))$

  D_1 … set of decisions of **original** program

  D_2 … set of decisions of **transformed** program

$\text{touches\_ID}(x, ID) \Rightarrow$

$IV_T(x) \subseteq ID \ \vee \ IV_F(x) \subseteq ID$

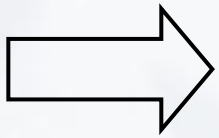
(coverage of x implies that at least one test vector is element of input data set ID)

Analysis of Code Transformations

- A code transformation potentially disrupts a given structural code coverage if it:
  - changes the reachability of statements or conditions
  - adds new control-flow paths into the program

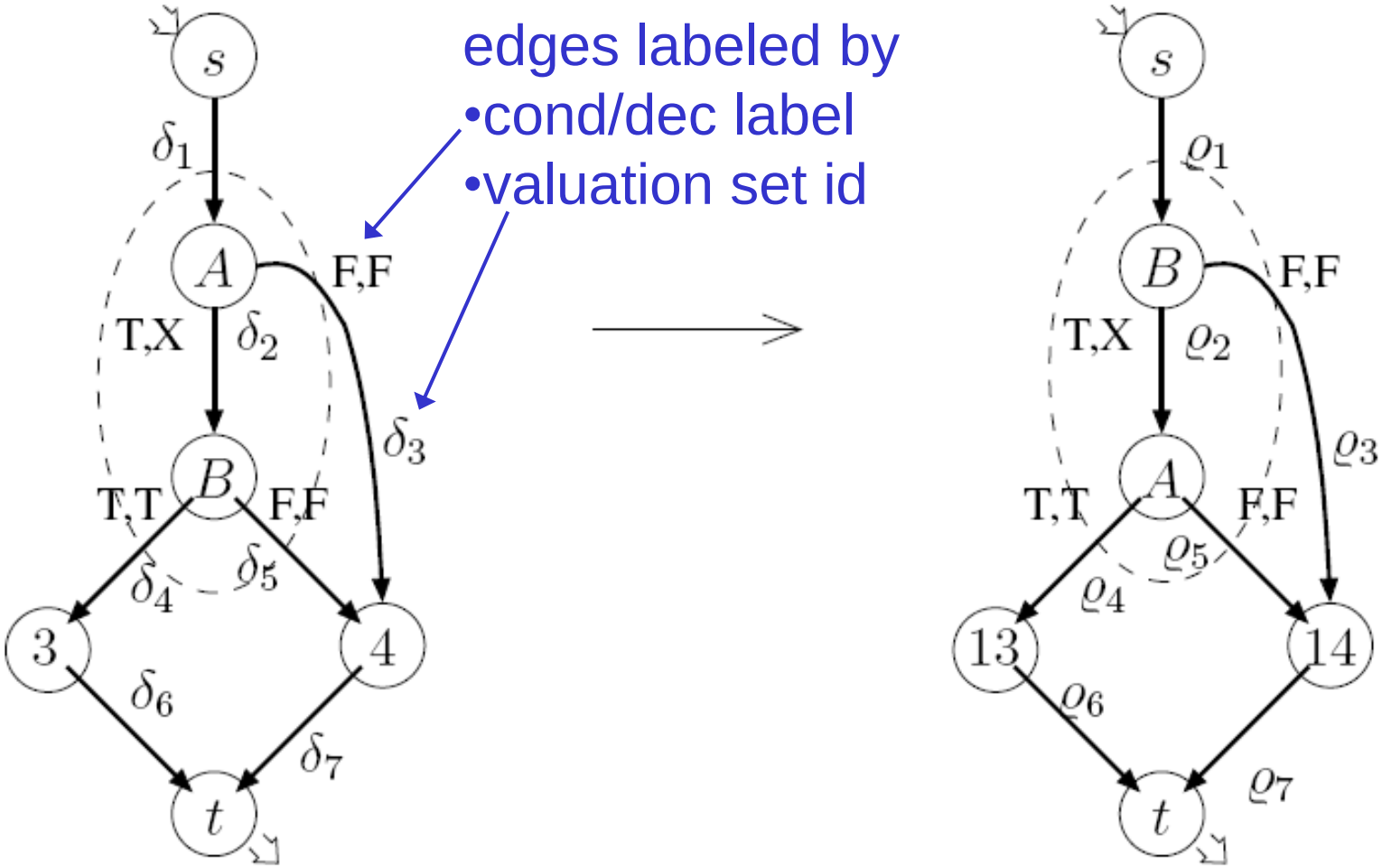
Example: Condition Reordering (with short-circuit)

```
1 if (A && B)
2    thenBlock
3 else
4    elseBlock
```

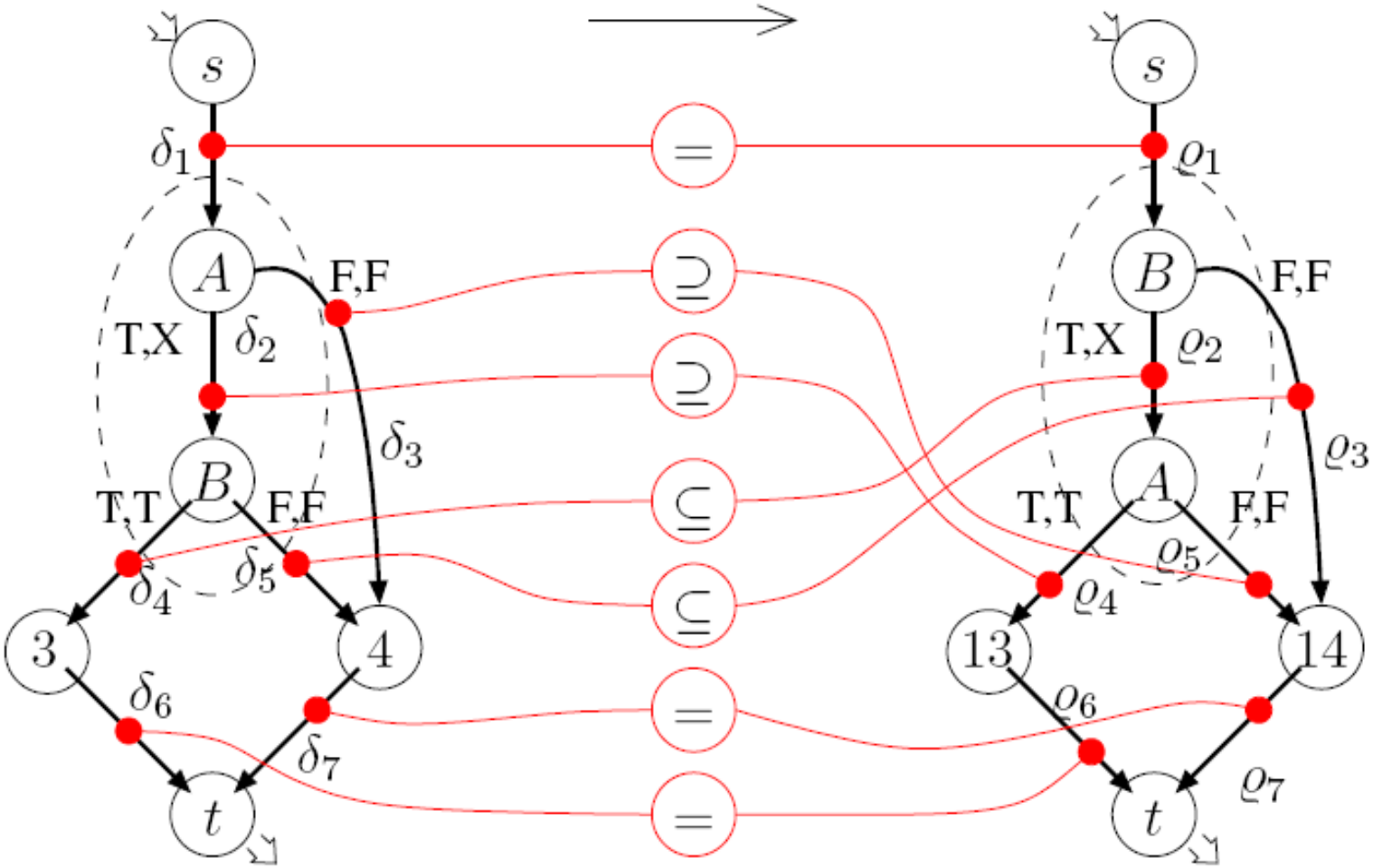


```
1 if (B && A)
2    thenBlock
3 else
4    elseBlock
```

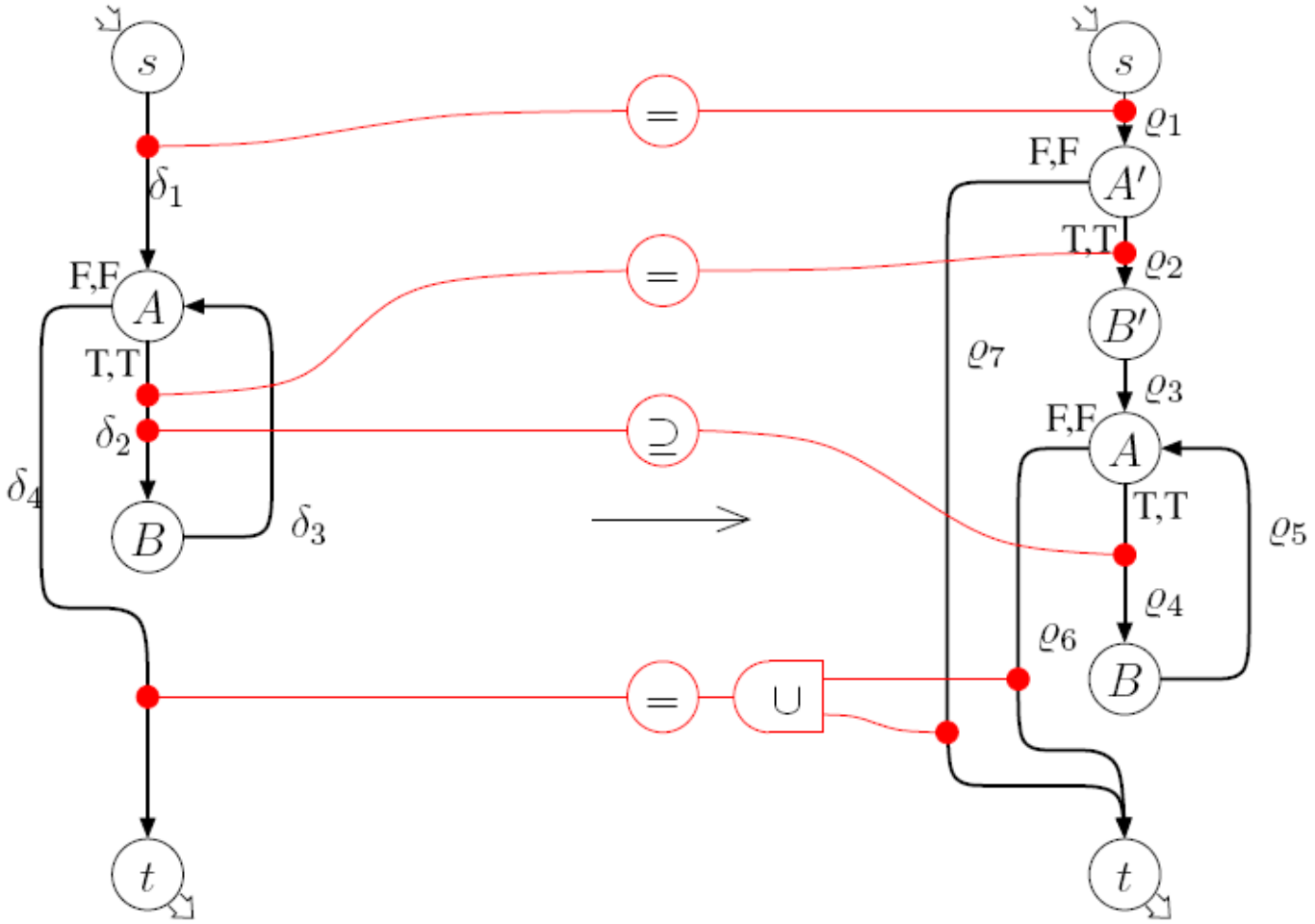
Structural Transformation of Condition Reordering (with short-circuit)



Transformation Relation for Condition Reordering (with short-circuit)



Transformation Relation for Loop Inversion



Results of Calculating Coverage Profiles

Transformation	SC	CC	DC
Condition reordering (without short-circuit)	✓	▪	✓
Condition reordering (with short-circuit)	✓	✓	✓
Loop peeling	▪	▪	▪
Loop inversion	✓	▪	▪

Future Work

- Modeling of additional (structural) code-coverage metrics (MCDC, scoped path coverage, …)
- Calculation of coverage profiles for additional code transformations
- Modeling of code transformations close to the concrete implementation (reduce cognitive complexity of modeling)

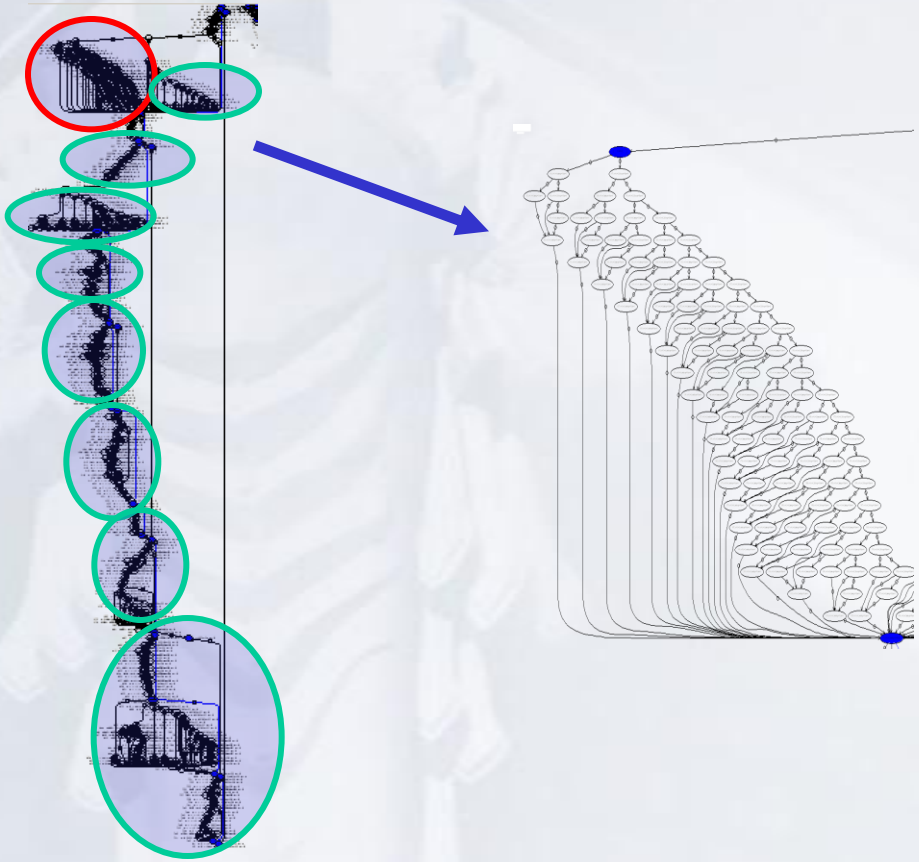
Further Reading

[1] Raimund Kirner, *SCCP/x - A Compilation Profile to Support Testing and Verification of Optimized Code*, In Proc. ACM Int. Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES'07), Sep./Oct. 2007, pages 38-42, Salzburg, Austria.

[2] Raimund Kirner and Susanne Kandl. *Test coverage analysis and preservation for requirements-based testing of safety-critical systems*. ERCIM News, (75):40–41, Oct. 2008.

[3] Raimund Kirner. *Towards preserving model coverage and structural code coverage*. EURASIP Journal on Embedded Systems, Hindawi, 2009.

MBTA: CFG Partitioning



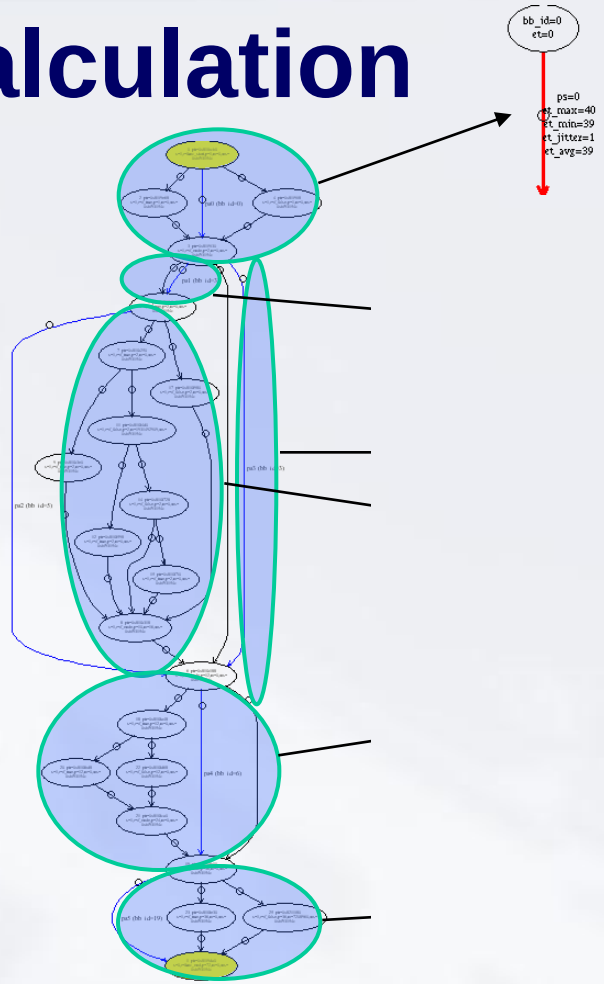
Example of generated code:

Entity	Value
#Paths	2.19e+32

(slide contributed by Ingomar Wenzel)

MBTA: WCET Bound Calculation

- Program segment execution times are combined by integer linear programming (ILP) or longest path search
- Advantage: only feasible paths within PS contribute
- Deficiency: lack of global path information ➲ refinement possible



(slide contributed by Ingomar Wenzel)