fortiss

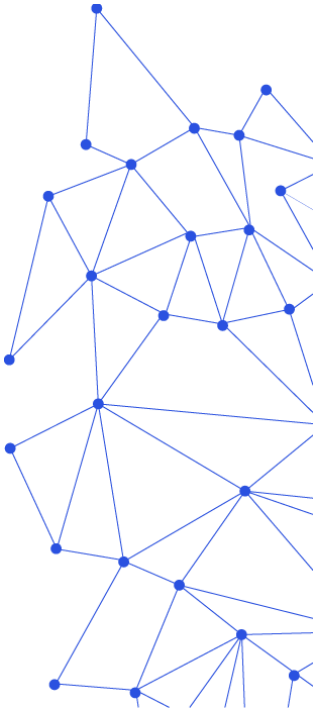
itemis

Using Language Engineering to Lift Languages and Analyses at the Domain Level

Daniel Ratiu, Markus Voelter, Bernd Kolb, and Bernhard Schaetz

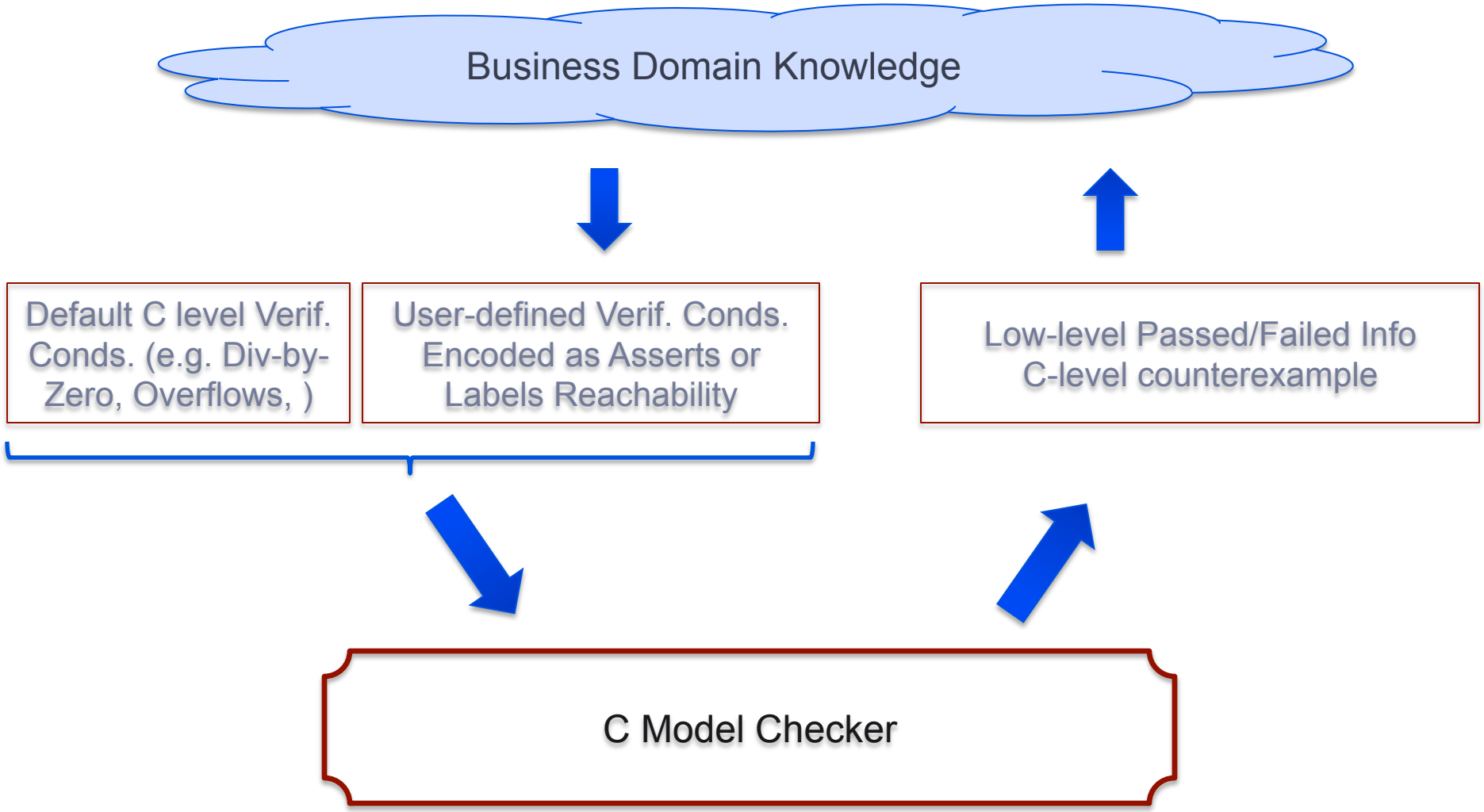
mbeddr

C the Difference. C the Future.



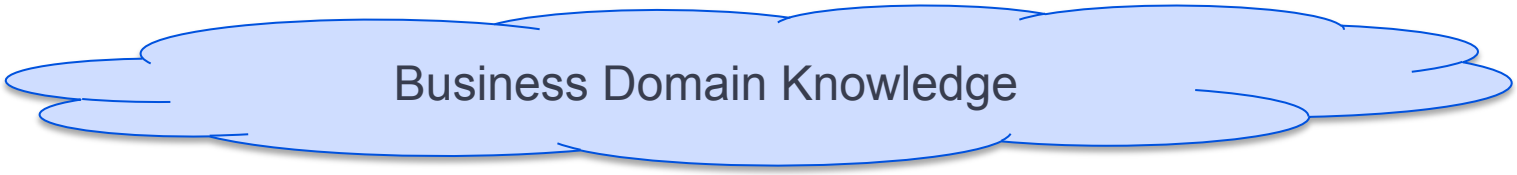
Users Perspective on Model Checking C Code

... Todays Status Quo



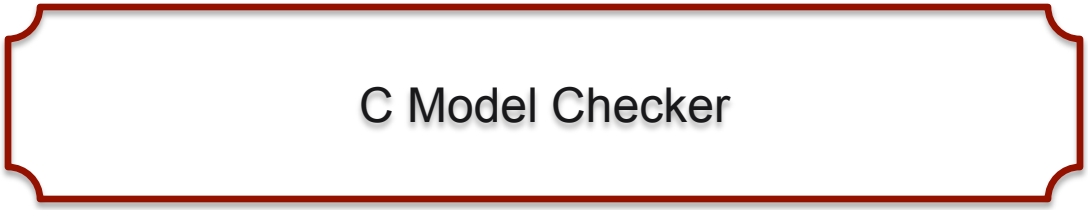
Users Perspective on Model Checking C Code

... Todays Status Quo



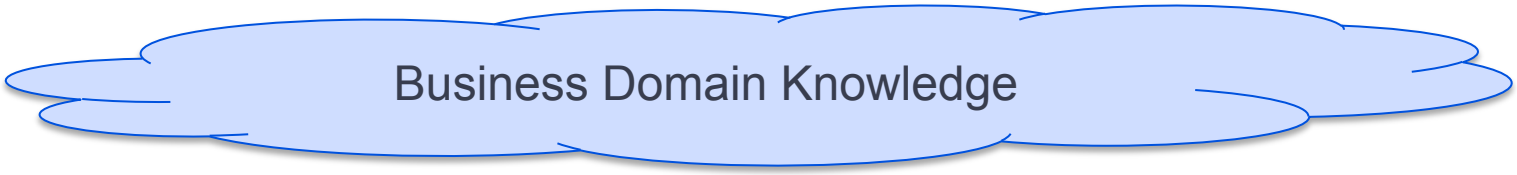
Hard to define advanced verification conditions

Hard to interpret the analyses results

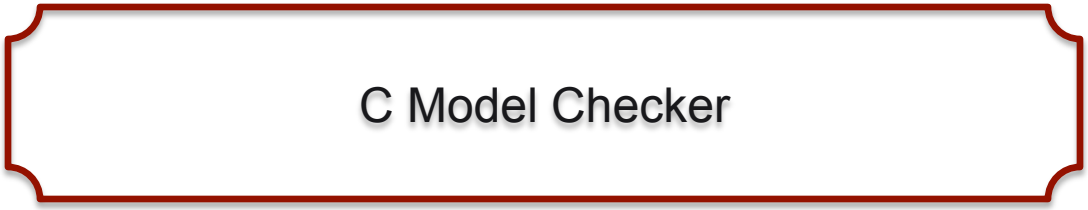


Users Perspective on Model Checking C Code

... Todays Status Quo



Modular and extensible languages help lifting the analyes closer to the domain.



High Level Language Extensions in MBEDDR

... Carry „Default“ Verification Conditions

```
mode computeNextMode(int16 x, mode prev) {
  return ERROR

} computeNextMode (function)
```

	x < 0	x >= 0
prev == MANUAL	AUTO	MANUAL
prev == AUTO	AUTO	MANUAL
prev == ERROR	ERROR	ERROR

„normal“
C code

decision table

Is this Decision Table Complete?

Is it Deterministic?

High Level Language Extensions in MBEDDR (2)

interfaces

components

„normal“
C code

```
cs interface SpeedComputer {
  void activate()
  void deactivate()
  float computeSpeed(int16 distance, int16 time)
}

component PlauzibilizedSpeedComputer extends nothing
  provides SpeedComputer speedComputer

  float lastSpeed = -1;
  boolean initialized = false;
  float maxPlausibleDelta = 10;

  void activate() <= op speedComputer.activate {
    initialized = true;
    return;
  } runnable activate

  void deactivate() <= op speedComputer.deactivate {
    initialized = false;
    return;
  } runnable deactivate
```

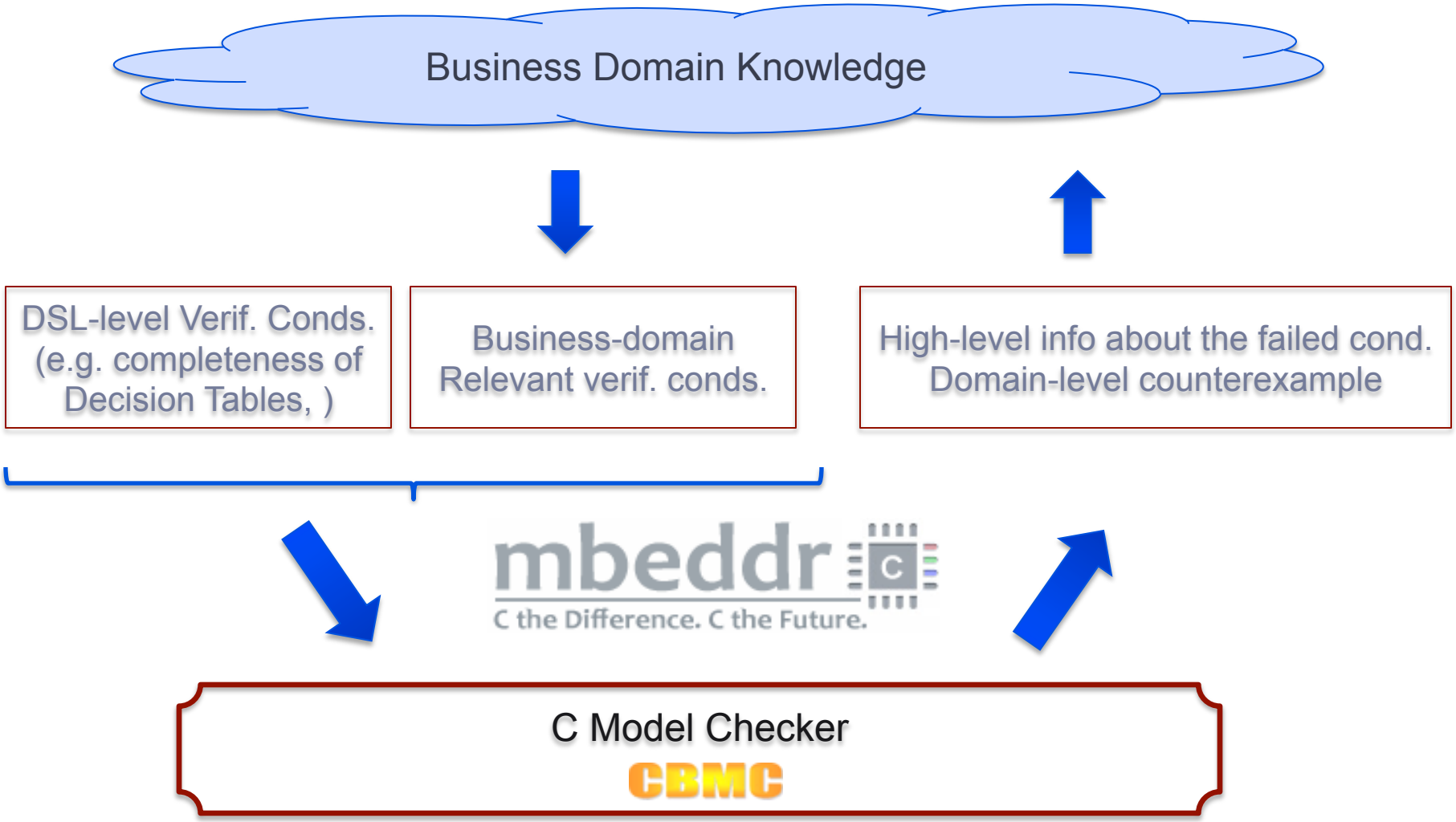
High Level Language Extensions in MBEDDR (2)

... Carry Business Domain Specific Verification Conditions

```
exported cs interface SpeedComputer {
  void activate()
    protocol init(0) -> new Active(1)
  float computeSpeed(int16 distance, int16 time)
    pre(0) time > 0
    pre(1) distance > 0
    post(2) result > 0
    protocol Active -> Active
  void deactivate()
    protocol Active -> init(0)
}
```

Define Pre-/Postconditions

Define Interface Protocol

Lifting Languages and Analyses at Domain Level

... with MBEDDR