Embedded Software Laboratory

RWTH AACHEN UNIVERSITY

Design-by-Contract for Embedded Systems

Jianmin Li

Shun Yang

RWTH Aachen

Design-by-Contract for Embedded Systems

- Motivation
- Design-by-Contract
- Our Idea and Goal
- Application Examples
- Future Work

Motivation

- Motivation
  - Embedded software is hardware-dependent: memory usage, battery power etc.
  - Embedded systems are interactive systems, which react to physical environment: network connectivity etc.
  - Growing number and complexity of hardware platforms and environment features

"Embedded systems are engineering artifacts involving computation that is subject to physical constraints which arise through interactions with the physical world" [T.A. Henzinger]

Motivation

⇒ A formal and precise specification of the physical constraints for software in embedded systems

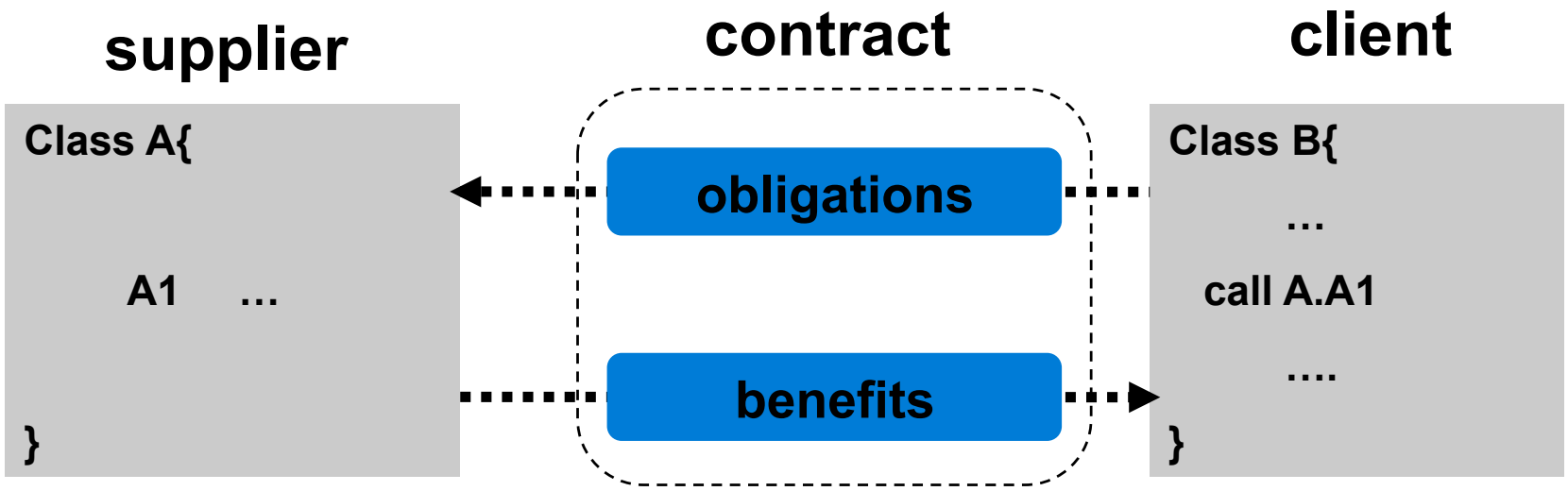
– Taking into account the variation of the underlying hardware und the environment in embedded systems

⇒ Improvement of the reliability when reusing software components

⇒ **Design-by-Contract (DBC)**

Definition of Design-by-Contract

- Design-by-Contract
  - A software engineering technology that utilizes runtime assertions to define precise verifiable interface specifications of the class with so-called invariants and pre- and post-conditions



Design-by-Contract

- Contract as Assertions
  - Precondition
  - Postcondition
  - Class Invariants

```
// @requires x >= 0.0
//@ensure x = result * result
Public  static double sqrt (double x) {
            …
}

// Invariants x ∈ ℜ && result >=0.0
```

Design-by-Contract

- The categorization of contracts in four levels [Beugnard et al.]
  1. Syntactic contracts
  2. Behavioral contracts
  3. Synchronization contracts
  4. Quality of service contracts

Our Approach

- Our Approach:

  „Extending assertions that deal with platform and environment features essential in embedded systems like battery power, localization, or memory and CPU consumption to support variation of these on different deployment targets.”

Application Example

- Video Podcast
  - Platform: Google Android
  - Playing a video from a RSS feed
  - Show the news of a RSS feed
  - Contracts about:

    network connectivity,

    battery,

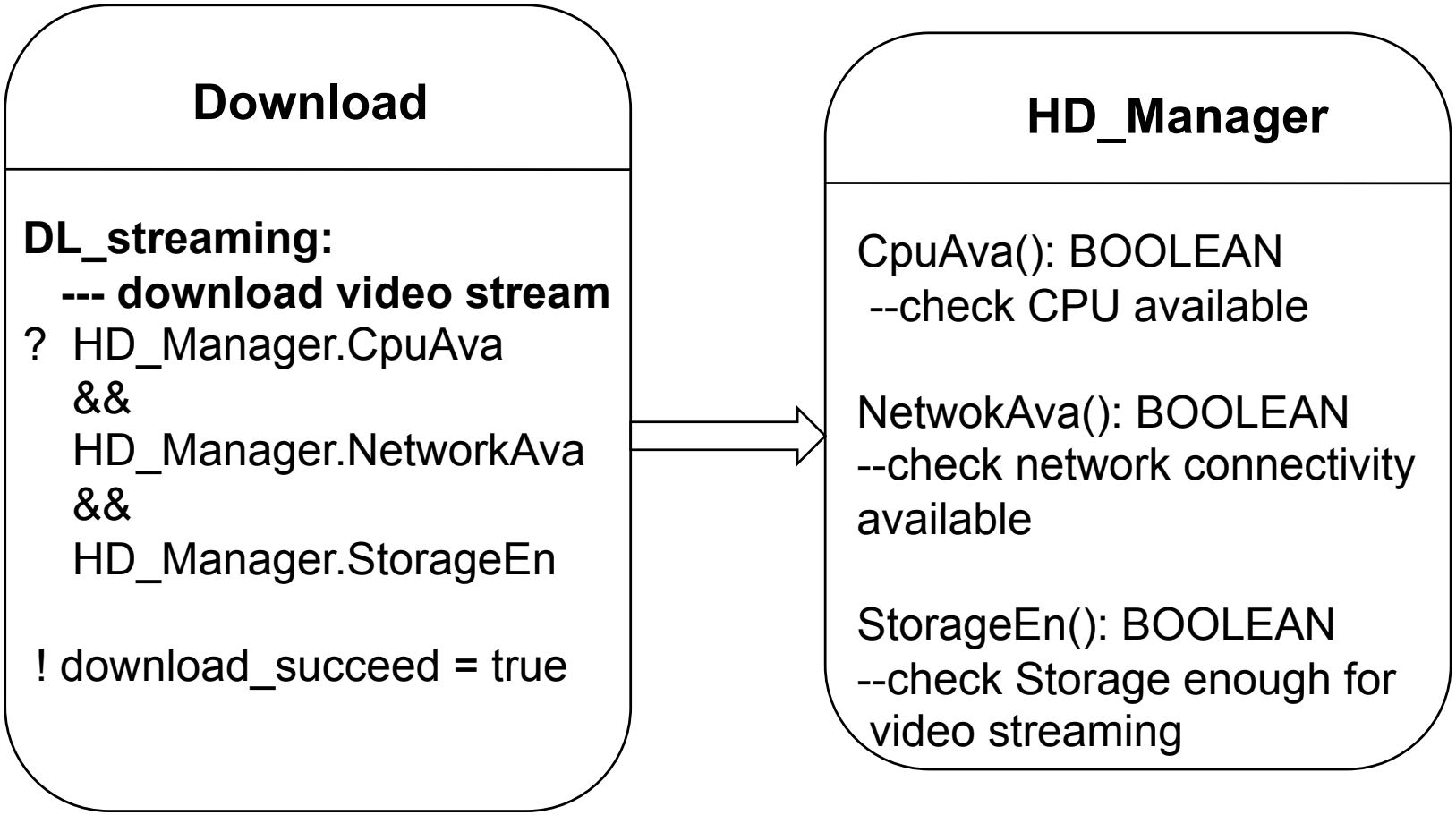
    storage,

    CPU load and availability

Android Emulator

Video Podcast

- Diagrams with pre-/postconditions



Future work

- Video Podcast is in processing
- No DBC support for Android
- Run time checking and static verification for Android

References

[1] T.A. Henzinger and J. Sifakis, „The embedded systems design challenge“, 2006

[2] A. Beugnard, J. J´ez´equel, N. Plouzeau, and D. Watkins, “Making Components Contract Aware,” 1999.

[3] Anil Kandrical “Design by Contract in den Programmier-sprachen C++, Eiffel und Java“, 2002

Embedded Software Laboratory

RWTH AACHEN UNIVERSITY

Thank you!

Questions?

Mail: jianmin.li@embedded.rwth-aachen.de