

Development of Safe and Reliable Embedded Systems using Dynamic Adaptation

Rasmus Adler, Daniel Schneider, Mario Trapp

Second Reader: Helge Parzyjegl

Why Dynamic Adaptation?

- > Embedded systems often deployed in fields where malfunctions are considered critical
 - > No catastrophic consequences → Safety
 - > Continuity of correct service → Reliability

- > Two different approaches

Redundancy

- > Adding sufficient devices to compensate failures
- > Higher degree of dependability
- > More expensive

Dynamic adaptation

- > Compensate failures by runtime adaptation
- > More flexibility
- > Less expensive

Evolution Stages

- > Stage 0 – non-adaptive systems
 - > System realizes no dynamic adaptation
- > Stage 1 – implicit adaptation
 - > Adaptation is modeled as indistinguishable part of the system's functionality
- > Stage 2 – explicit adaptation
 - > Adaptation behavior is explicitly considered and modeled
 - > Existence of a runtime adaptation framework
- > Stage 3 – Software engineering of adaptive systems
 - > Existence of design and development methodology
 - > Support for analysis, validation, verification, reuse, automatation ...

Building Blocks?

“An approach to ensure correctness of component based adaptation“

“A formal model of reconfiguration and an associated set of high level general system dependability properties”

“Containment Units monitor the quality of functionalities”

“RoSES deals with product family architectures realizing dynamic reconfiguration”

“EASL deals with transitions between configurations”

“Linear temporal logic is extended with an adapt operator”

“Constructing and verifying adaptation models using petri nets”

Conclusions

Where are methodologies?

- > We are at stage 2 and only approaching stage 3
- > Methodologies need
 - > Common understanding of terms (e.g., adaptivity)
 - > Much experience from many different approaches