Model Based and Certified Automotive Software Development:
Increased Safety & Security
Agenda

• Automotive Software Development
  • Goals

• Model Based Development Process
  • Single Source
  • Domain Specific Modeling
  • Automatic Code Generation

• Certification

• Summary
Automotive Software Development

Goals

- Goals -> significant improvements in the areas of:
  
  - Quality/Safety/Security
  
  - Efficiency/Productivity/Cost
  
  - Time-to-market
Agenda

- Automotive Software Development
  - Goals

- Model Based Development Process
  - Single Source
  - Domain Specific Modeling
  - Automatic Code Generation

- Certification

- Summary
Model Based Development Process
Design Independent of Development Stage

Model based / abstracted development
- Target independent functional specification

Network of Functions

V-Cycle stage dependent Development Targets

PC
Rapid Prototyping
ECU

f: Function
m: Function Module
Model Based Development Process
Target Independent Design

Model based / abstracted development
- Target independent functional specification
Model Based Development Process
Support of Variants

Model: Single Source

Various experiments
Various data sets
Various implementations
Model Based Development Process

Single Source Models

Key for safety and security:

**Single Source Models**

Applicable to multiple V-cycle stages:
range of targets (PC, RP, ECU’s)

Handling of variants through:
multiple experiment configurations
multiple data sets
multiple implementation specifications
Agenda

- Automotive Software Development
  - Goals

- Model Based Development Process
  - Single Source
    - Domain Specific Modeling
  - Automatic Code Generation

- Certification

- Summary
Model Based Development Process

Productivity Increase Through Domain Specific Modeling

• “The entire history of software engineering is that of the rise in levels of abstraction”

• New programming languages do not increase productivity

• UML and visualization of code has not increased productivity

• Abstraction of design work can be raised to domain level

Number of new product features implemented in a given time

** Software Productivity Research & Capers Jones, 2002

MetaCase
J.-P. Tolvanen, 2006
Model Based Development Process
Automotive Domain Specific Modeling 1/2

**SW-Architecture and Design** to assure safe implementation and re-use

- Definition of Modules (SW Components), Classes (Services), Processes (Runnable Entities) and Messages (Ports) enable focus on:
  - functional behavior
  - interactions of atomic pieces
  - abstraction of timing

- Definition of SW elements which are relevant for automotive ECUs, like:
  - variable, parameter, constant, class, module, process, message vs. control theory relevant elements
  - formula, 1D- and 2D-tables, distributed 1D- and 2D-tables
  - separate memory classes for NVRAM, e. g. for self learning algorithms
Real-time Architecture and Design assuring correct real-time behavior

- Definition of tasks and scheduling
  - timing/activation based on system constraints
  - trade-off between performance and timing needs

Implementation Specification to adapt the SW-model to the specific μC

- Definition of bit resolution, limits, conversion formulas, memory location, naming conventions – enables target specific efficiency of implementation

Standardization activities

- Autosar, ASAM, OSEK, …
Agenda

• Automotive Software Development
  • Goals

• Model Based Development Process
  • Single Source
  • Domain Specific Modeling
    ➢ Automatic Code Generation

• Certification

• Summary
Model Based Development Process
Auto-Codegeneration

Increased quality and reduced development time through:

- Increased productivity
- Optimization for individual µC’s

- Shift review from code level to abstract model layer
- Reduced implementation errors

- Consistency of generated artifacts (ASAM file, Autosar template …)
- Single source development of new requirements
  (MISRA styles, Autosar, new targets)
- Consistency across targets (PC-, RP- and µC)
Agenda

• Automotive Software Development
  • Goals

• Model Based Development Process
  • Single Source
  • Domain Specific Modeling
  • Automatic Code Generation

• Certification

• Summary
Certification

Overview

Processes *:

- ISO/IEC 12207 commercial
- ISO/IEC 15288
- Automotive SPICE (s. Metz, Schedl)
- IEC 61508 (s. Glötzner)

Why:

- Quality improvements (best engineering practices)
- Risk minimization (liability)

Prerequisite:

- In-house Software development process is rated (certified) by an independent institute

* TÜV NORD, G. Glöe, 2006
Certification

IEC 61508

Functional safety of electrical / electronic / Programmable electronic safety related Systems

Die IEC 61508 beschreibt “die im Verkehr geschuldete Sorgfalt” zur Sicherheit von Embedded Systemen.
Agenda

• Automotive Software Development
  • Goals

• Model Based Development Process
  • Single Source
  • Domain Specific Modeling
  • Automatic Code Generation

• Certification

• Summary
Summary

Goals - significant improvements in the areas of:

- Quality/Safety/Security
- Efficiency/Productivity/Cost
- Time-to-market

Measures to meet the goals:

- Domain specific, model based development process
- Automatic code generation
- Certified tools and processes
Questions ?