

ETAS

LiveDevices  
ETAS Group

Vetronix  
ETAS Group



Dr. Ulrich Lefarth, ETAS GmbH

# 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

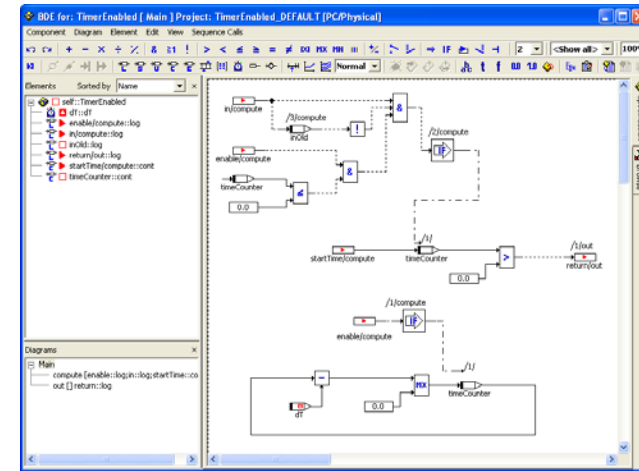
# Agenda

- Automotive Software Development
  - Goals
- Model Based Development Process
  - Single Source
    - Domain Specific Modeling
    - Automatic Code Generation
- Certification
- Summary

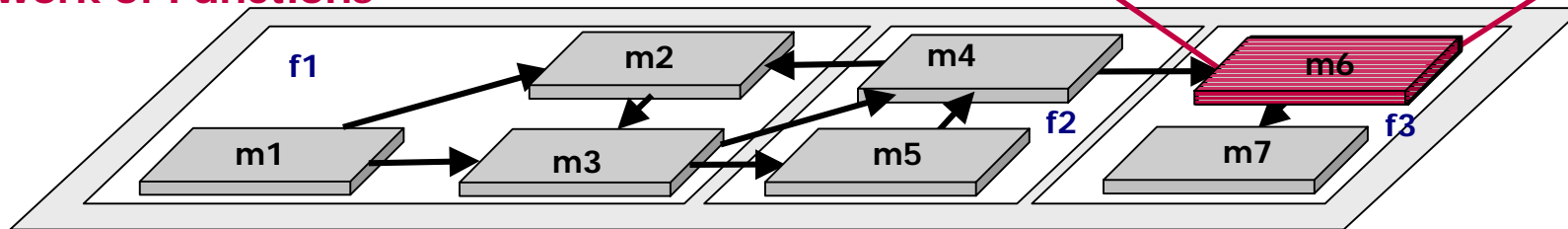
# Model Based Development Process

## Design Independent of Development Stage

Model based / abstracted development  
 - Target independent functional specification

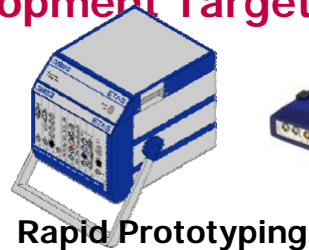
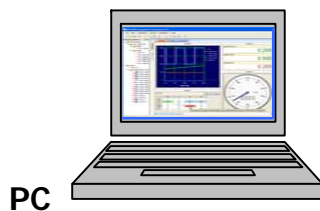


### Network of Functions



f: Function  
 m: Function Module

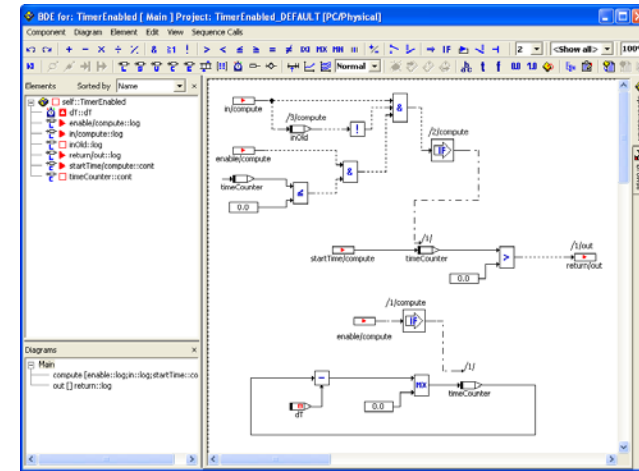
### V-Cycle stage dependent Development Targets



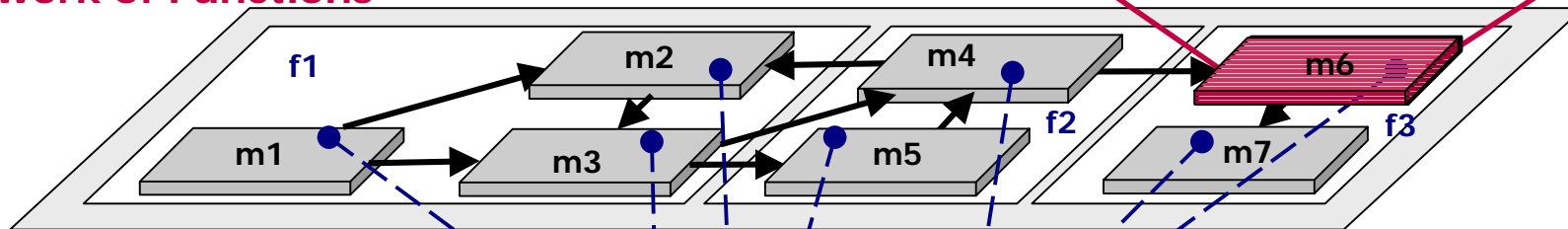
# Model Based Development Process

## Target Independent Design

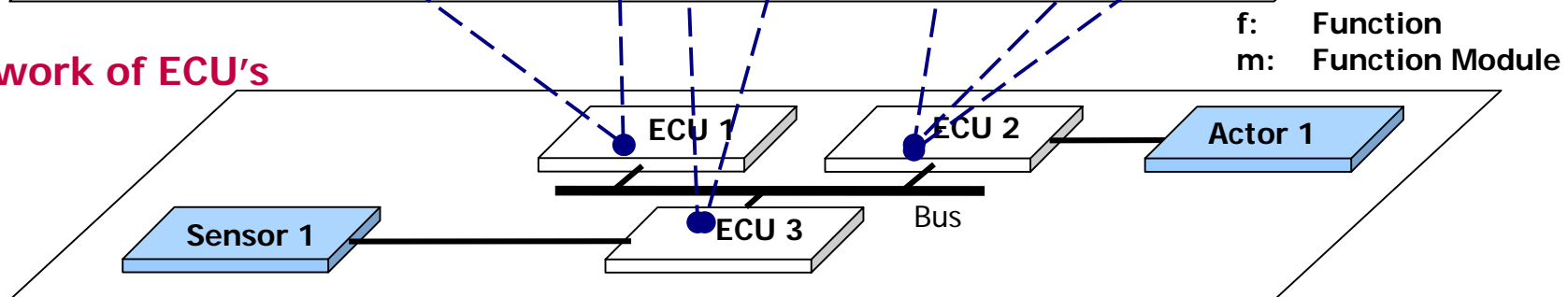
Model based / abstracted development  
 - Target independent functional specification



### Network of Functions



### Network of ECU's



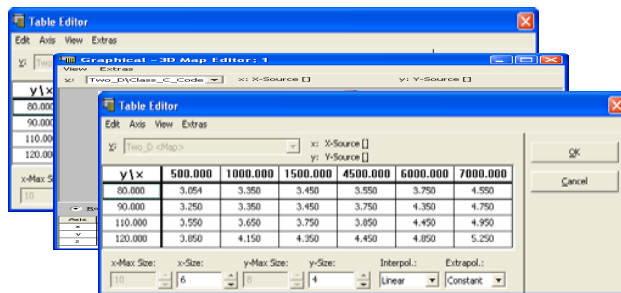
# Model Based Development Process

## Support of Variants

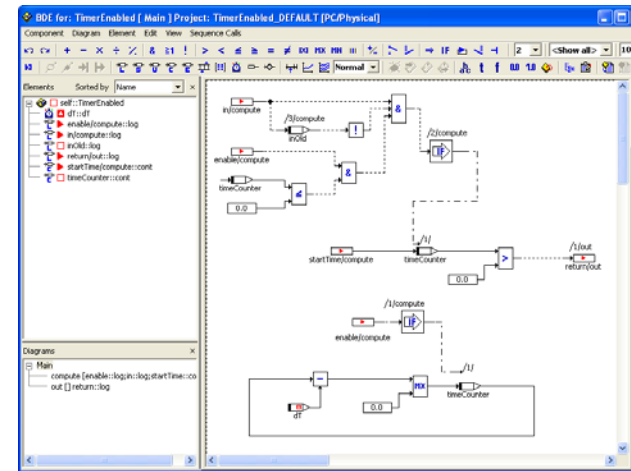
Various experiments



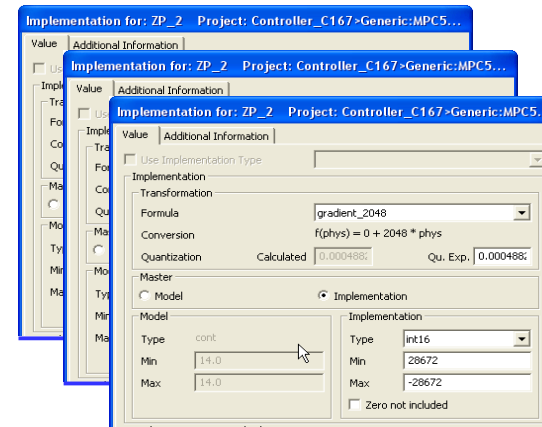
Various data sets



## Model: Single Source



Various implementations



# Model Based Development Process

## Single Source Models

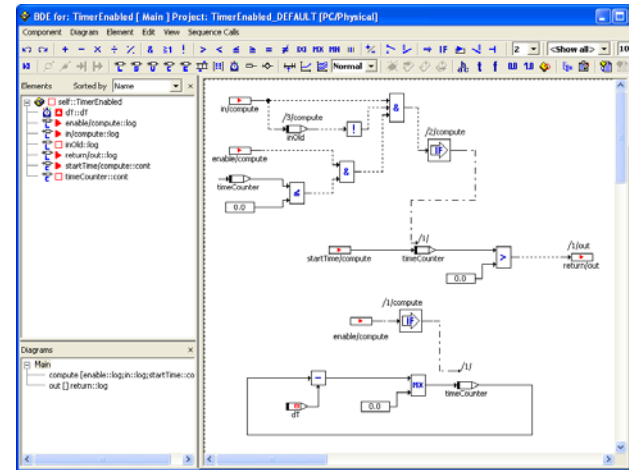
Key for safety and security:

## 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





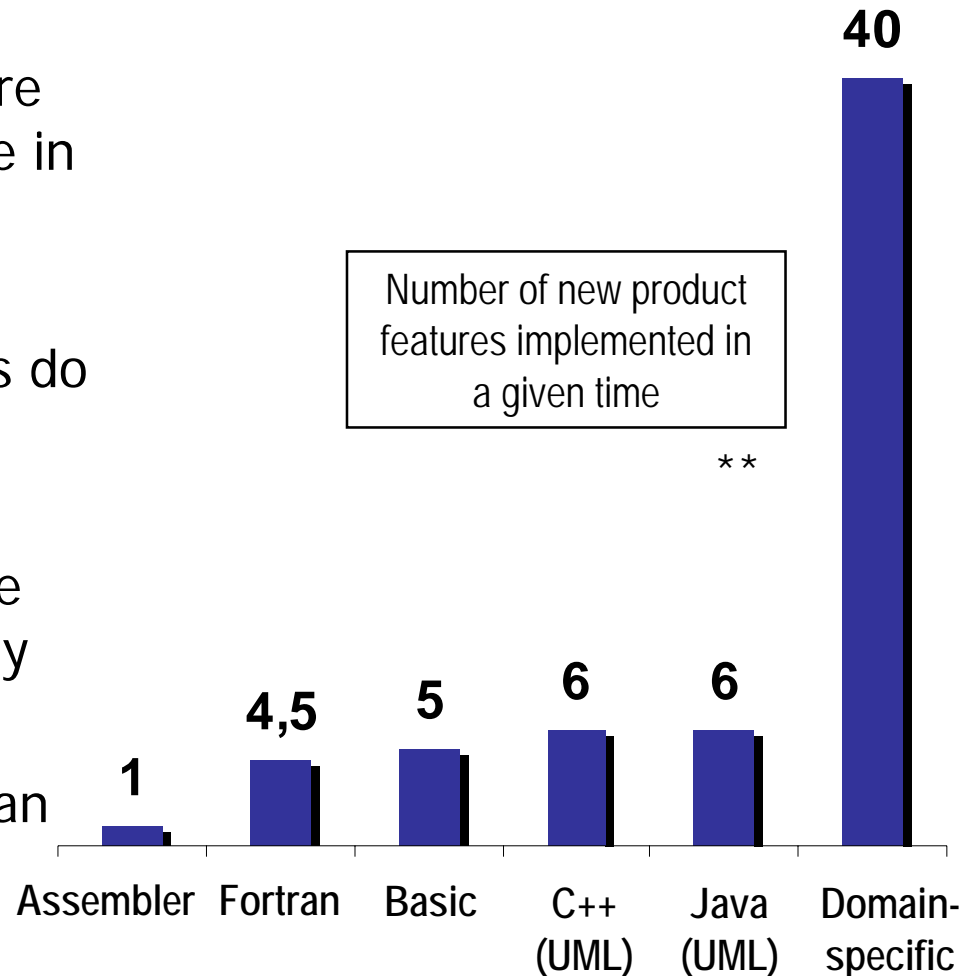
# Agenda

- 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



MetaCase  
J.-P. Tolvanen, 2006

\*\* Software Productivity Research &  
Capers Jones, 2002

# 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

# Model Based Development Process

## Automotive Domain Specific Modeling 2/2

### 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 $\mu\text{C}$

- 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  $\mu\text{C}$ '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  $\mu\text{C}$ )

# 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.

**TÜV Nord e.V. SEECERT**  **Große Bahnstraße 31  
D-22525 Hamburg**

Software & Elektronik Zertifizierungsstelle

**ZERTIFIKAT** **CERTIFICATE**  
Konformitätsbescheinigung *Certificate of Conformity*

**Registrier-Nr.**  
Registered No.  
**H.SEE.02.002-02**

Zeichen des Auftraggebers <small>Reference of Applicant</small>	Auftragsdatum <small>Date of Application</small>	Aktenzeichen <small>File Reference</small>	Prüfbericht-Nr. <small>Test Report No.</small>
4500385257-924	2002-03-27	CER	H.SEE.02.002.10.TL3

**Name und Anschrift der Firma**  
Bearer of Certificate

**ETAS GmbH**  
Borsigstraße 14  
D-70469 Stuttgart

Der unten genannte Codegenerator der oben genannten Firma ist für SIL3-Anwendungen im Automotive-/Schienenfahrzeug-Bereich geeignet ('fit for purpose'). Die zugehörigen Dokumente lagen der Zertifizierungsstelle vor. Die enthaltenen Angaben stimmen mit dem Produkt überein.

<b>Produkt</b> <small>Product</small>	ASCET-SD – Codegenerator
<b>Typenbezeichnung</b> <small>Type Description</small>	V4.1.1 Inkl. TIP-Knorr V4.1.8
<b>Geprüft nach</b> <small>Tested in Accordance with</small>	'Fitness for Purpose' in Anlehnung an IEC 61508-1 [1998-12] und IEC 61508-3 [1998-12] (SIL3)
<b>Geltungsdauer des Zertifikats</b> <small>Validity of Certificate</small>	2004-05-31

**TÜV NORD SEECERT** **Hamburg, 2002-05-31**  
Software & Elektronik Zertifizierungsstelle dated

**DAR-Registrierungsnummer: DAT-ZE 012/00-10** **Der Leiter:**   
Registration No. of Certification Body Head of Certification Body

Hinweis: Das Zertifikat gilt nur für die genannte Firma und das bezeichnete Produkt.  
Jede beabsichtigte oder vorgenommene Änderung ist der Zertifizierungsstelle anzuzeigen.

# 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 ?