



Powertrain Engineering Developments and the Autocode Dilemma

Shane Davies

Ricardo Tarragon

IEE CarTronics Seminar

Cambridge, 4th December 2003

- ❑ **Modern vehicle electronics and X-by-wire**
- ❑ **Model based development and automatic code generation**
- ❑ **Automatic code generation for X-by-wire and safety-critical systems**
- ❑ **Conclusions**

- Modern vehicle electronics and X-by-wire**
- Model based development and automatic code generation**
- Automatic code generation for X-by-wire and safety-critical systems**
- Conclusions**

Modern vehicle electronics and X-by-wire

Trends in vehicle electronics

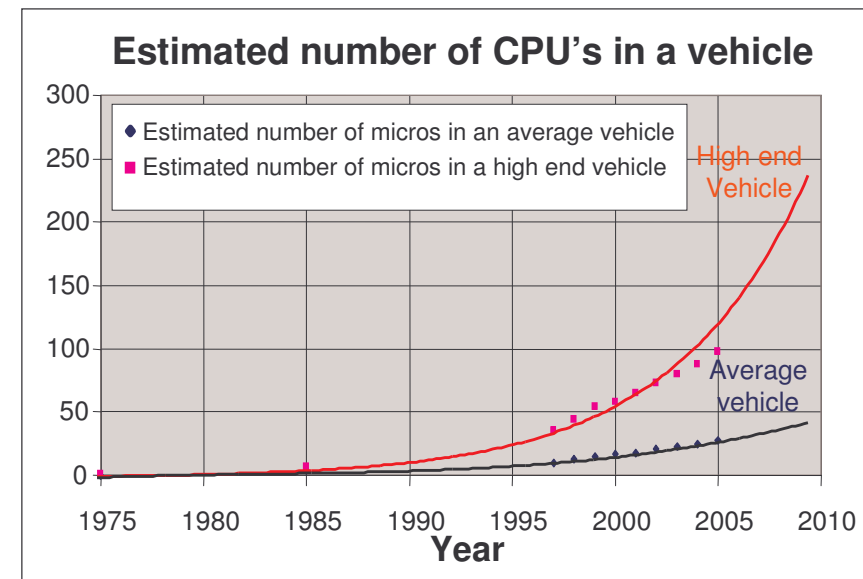


Industry trend is for:

- ❑ Increased number of micros on-vehicle.
- ❑ Distributed micros with network communications.
- ❑ Increased use of Infotainment systems.
- ❑ Communication with external sources.
- ❑ Introduction of X-by-wire.



- ❑ Increased component interaction.
- ❑ Increased software complexity.
- ❑ Increased safety requirements.



Modern vehicle electronics and X-by-wire

X-by-Wire



The process of removing a direct mechanical linkage between the driver and the various systems in the vehicle.

- ❑ Throttle by wire – throttle cable replaced with pedal sensor and electronic throttle.
- ❑ Shift by wire – stick shift replaced with electronic gearbox, e.g. Tiptronic gearbox.
- ❑ Brake by wire – hydraulics replaced with brake sensor and actuators at the wheels.
- ❑ Steer by wire – steering column and hydraulics replaced with electronic steering and actuators.

Benefits

- ❑ Integrated vehicle control.
- ❑ Less bulky components.
- ❑ Removal of steering column for steer by wire.

Drawbacks

- ❑ Safety-critical and lots of interaction therefore difficult to define “safe” conditions.
- ❑ Requires built-in redundancy and fault tolerant comms to ensure safe operation.

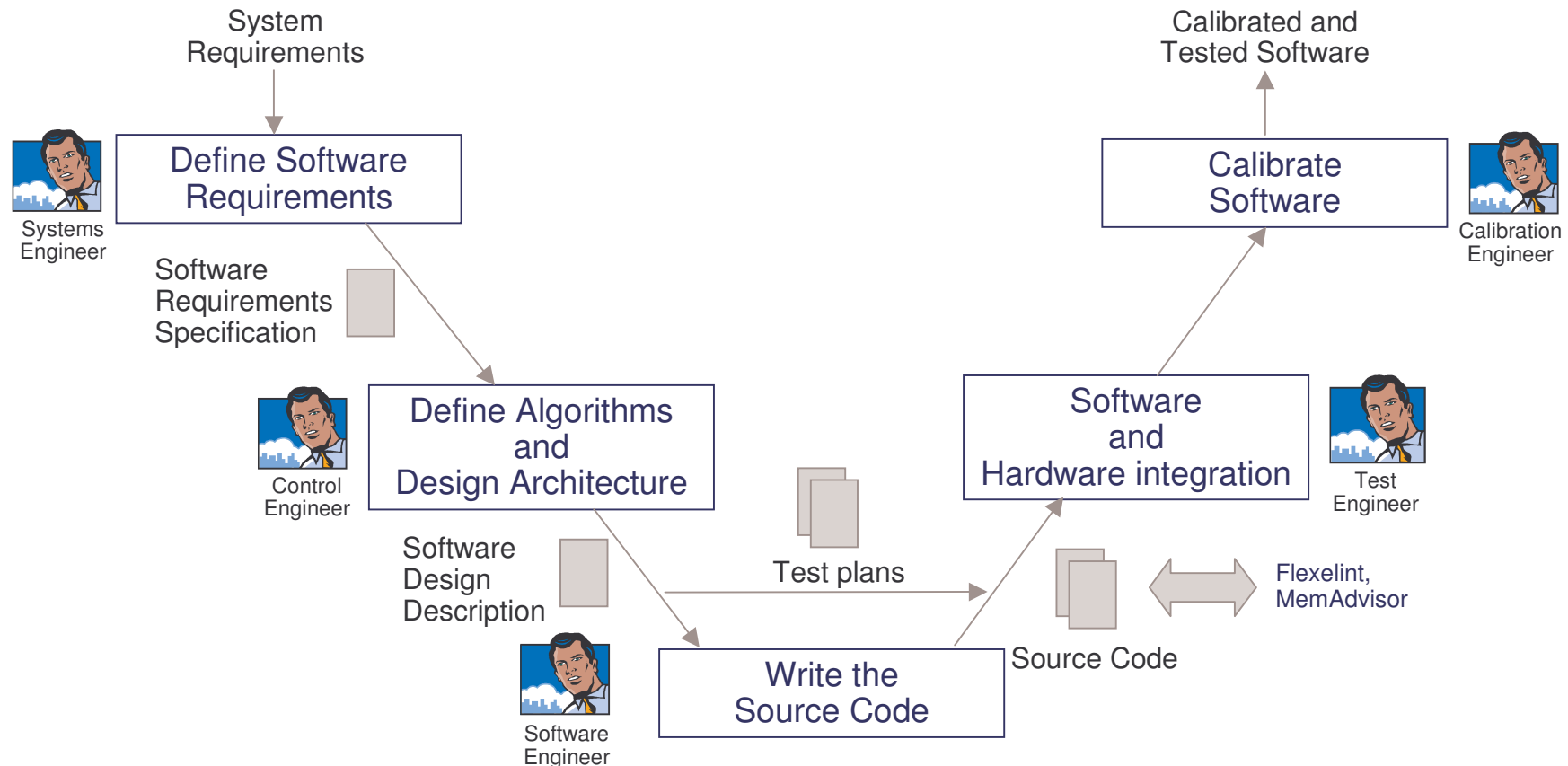
Top of the range car has more computing power on board than a 1982 Airbus A310 commercial aircraft!

To manage the extra software complexity the industry has had to evolve the software development process.

- Modern vehicle electronics and X-by-wire
- Model based development and automatic code generation
- Automatic code generation for X-by-wire and safety-critical systems
- Conclusions

Model based development and automatic code generation

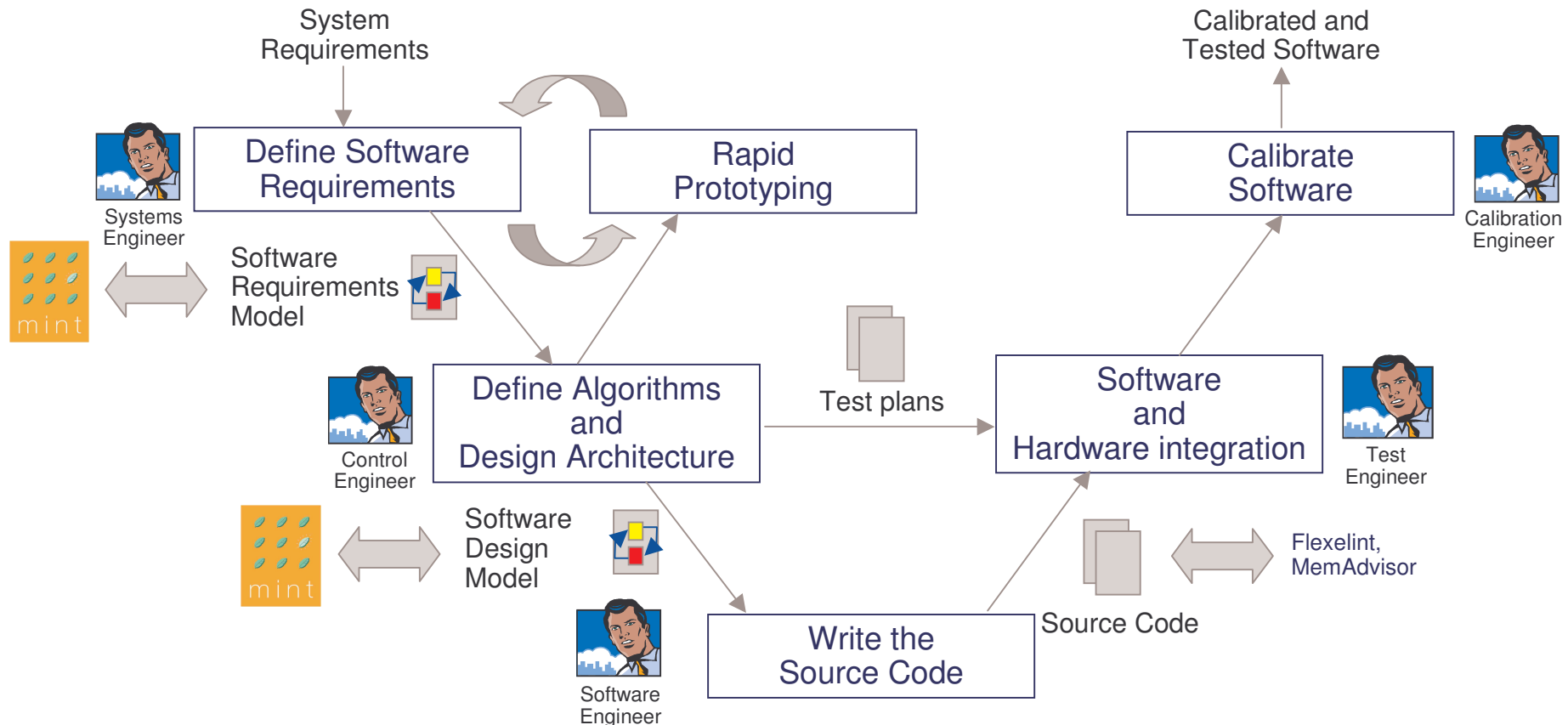
Traditional software development process



- ❑ Document driven.
- ❑ Source code often the reference for bug fixes.
- ❑ Code is reviewed against “automotive” industry guidelines – MISRA-C.
- ❑ Commercial tools such as Flexelint and MemAdvisor used to check the structure and correctness of the code.
- ❑ Test plans driven by the code and generated during or after the code is written.

Model based development and automatic code generation

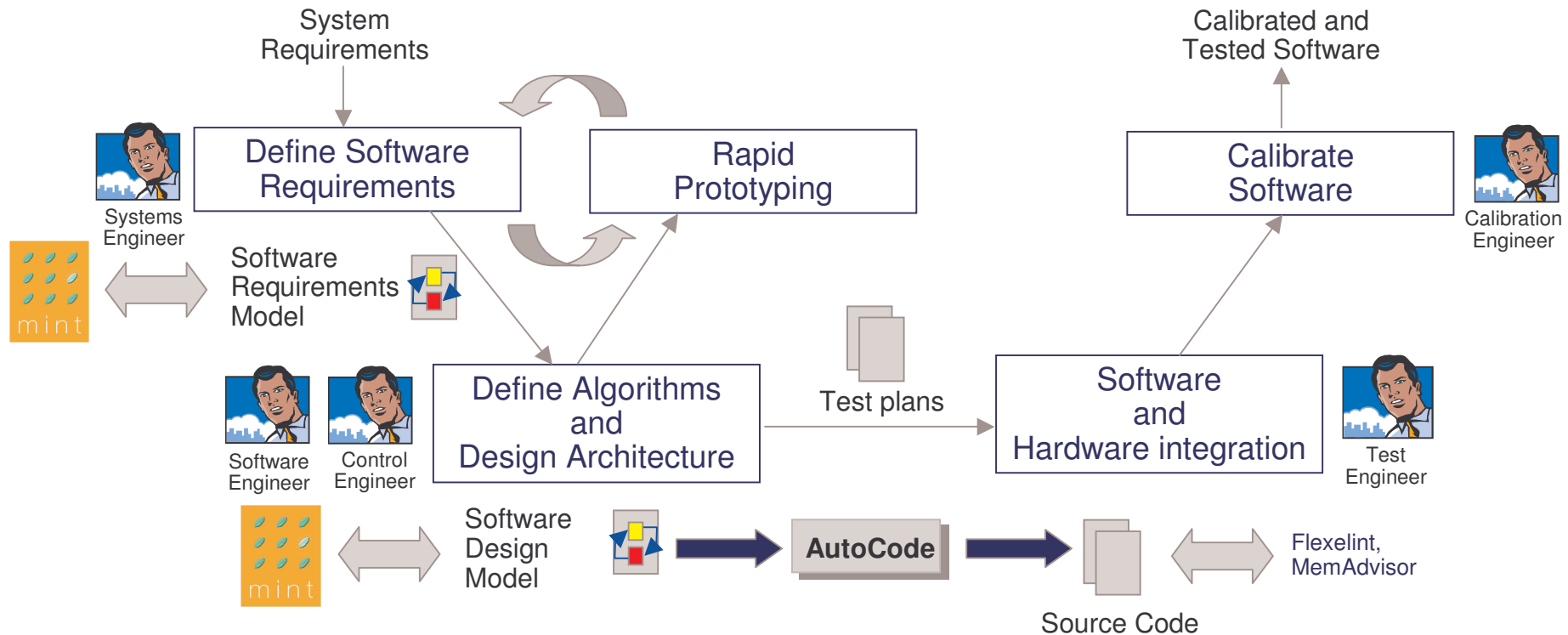
Model based development process



- ❑ Model driven.
- ❑ Design and requirements model is the reference for updates.
- ❑ Model is reviewed against “automotive” industry guidelines – MAAB.
- ❑ Commercial tools such as **mint** used to check the style, structure and correctness of the models.
- ❑ Test plans generated from the requirements model and test vectors applied to the design model and the code.

Model based development and automatic code generation

Automatic code generation



- ❑ Manual coding step is replaced by an auto-coder.
- ❑ Software engineer moves up the food chain and works with the control engineer to develop the design model.

Model based development and automatic code generation



- ❑ Developers can work in the modelling domain using powerful simulation tools.
- ❑ A generic simulation model can be configured for different targets.
- ❑ The configuration is defined at a high level within the autocode tool.
- ❑ The manual coding step is replaced by the autocoder (although manual coding only really accounts for ~10% of the development costs anyway).
- ❑ Removes the chance of a software engineer misinterpreting the design model.

However:

- ❑ Removing the manual code step also removes a level of sanity checking on the design.
- ❑ There's a lack of industry standards defining how model constructs are represented in code.
- ❑ Code generators have historically produced difficult to understand, unreadable code...this is however something that's improved a lot in the last 12-18 months.

- ❑ Modern vehicle electronics and X-by-wire
- ❑ Model based development and automatic code generation
- ❑ Automatic code generation for X-by-wire and safety-critical systems
- ❑ Conclusions

Dilemma in using automatic code generation for X-by-wire and safety critical systems



- ❑ MISRA (Motor Industry Software Reliability Association) has produced a set of “Guidelines for the use of the C language in vehicle-based software”.
- ❑ Commonly referred to as “MISRA C” it’s been an industry standard for automotive software development since 1998.
- ❑ The definition of “MISRA C” took the industry over 10 years.
- ❑ MISRA also defines categories for safety related failures in vehicle, Safety Integrity Levels, rated 0 to 4 with 4 being the highest.

Dilemma in using automatic code generation for X-by-wire and safety critical systems



SIL level definitions:

Controllability Categories	Definition	SIL
Uncontrollable	This relates to failures whose effects are not controllable by the vehicle occupants, and which are most likely to lead to extremely severe outcomes. The outcome cannot be influenced by a human response.	4
Difficult to Control	This relates to failures whose effects are not normally controllable by the vehicle occupants but could, under favourable circumstances, be influenced by a mature human response. They are likely to lead to severe outcomes.	3
Debilitating	This relates to failures whose effects are usually controllable by a sensible human response and, whilst there is a reduction in the safety margin, can usually be expected to lead to outcomes which are at worst severe.	2
Distracting	This relates to failures which produce operational limitations, but a normal human response will limit the outcome to no worse than minor.	1
Nuisance Only	This relates to failures where safety is not normally considered to be affected, and where customer satisfaction is the main consideration.	0

Definition of Controllability Categories [MISRA 1994]

Most X-by-wire systems by their nature are classed as SIL 3 and above.

Dilemma in using automatic code generation for X-by-wire and safety critical systems



- ❑ Autocoders such as dSPACE TargetLink and Ascet-SD claim to support “MISRA C” up to SIL3 but this is often with non-compliances.
- ❑ The Mathworks Automotive Advisory Board, MAAB, have defined a set of guidelines for model based development but they are really just a starting point.
- ❑ It will take years before modelling and autocode tools reach the same level of maturity as “MISRA C”.
- ❑ In removing the manual coding step from the process we are missing an extra level of review and ultimately the code being output is only as good as the model being input.

Garbage In → Garbage Out

- ❑ **Modern vehicle electronics and X-by-wire**
- ❑ **Model based development and automatic code generation**
- ❑ **Automatic code generation for X-by-wire and safety-critical systems**
- ❑ **Conclusions**

Conclusions



- ❑ Model based development and autocoding provide a big advancement in the process of developing automotive software.
- ❑ Autocode tools are making big steps forward in satisfying industry coding standards and ensuring code is readable and easy to review against a model.
- ❑ However with the advent of X-by-wire systems there is a more rigorous demand on software reliability as they are by nature safety critical.
- ❑ Autocode tools are not yet at a level of maturity to provide confidence that they satisfy the extra demands for software reliability required for X-by-wire.
- ❑ By the time X-by-wire is commonplace in production, 3 to 5 years, autocode tools will have reached the required level of maturity to satisfy the increased demands for safety.