Discussions on moving toward with Assuring Dependability of Consumer Devices RFP

June 22nd, 2012

Akira Ohata

TOYOTA MOTOR CORPORATION

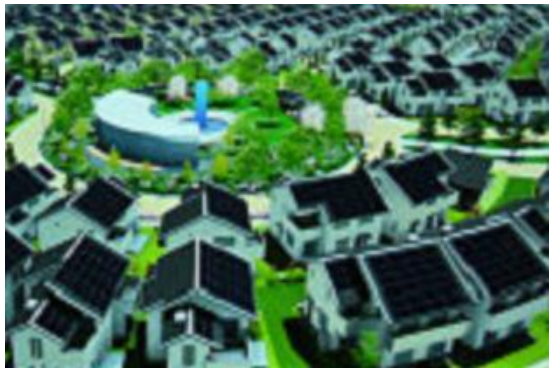
Contents

1. Review of RFI assuring dependability for consumer devices
2. Responses for RFI
3. Moving toward RFP
4. Result of System Assurance Task Force (SysA)

Contents

1. Review of RFI assuring dependability for consumer devices
2. Importance of prove in use
3. Responses for RIF
4. Moving toward RFP
5. Result of System Assurance Task Force (SysA)

Industrial and Consumer Devices



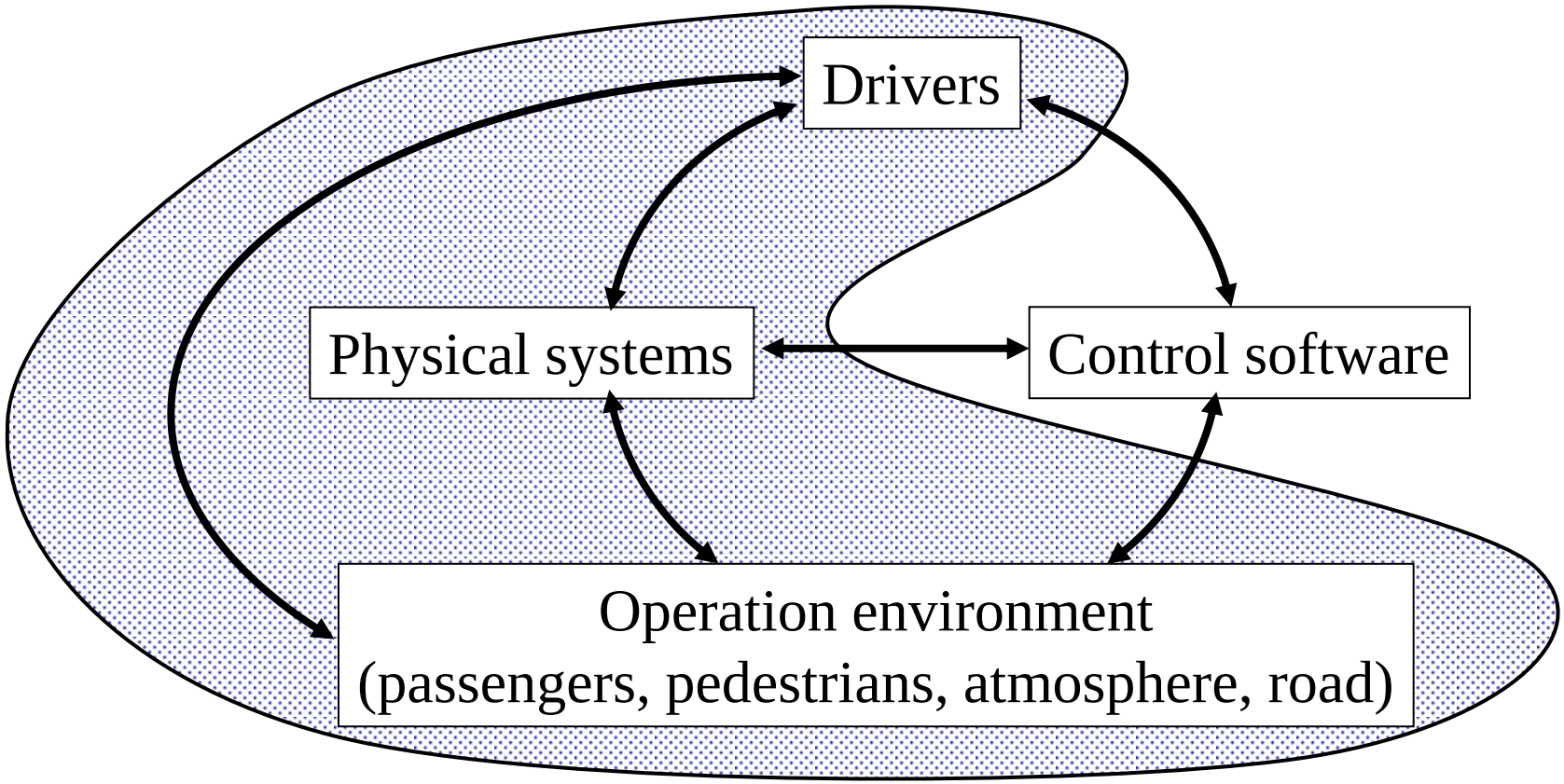
Industrial Devices

Consumer Devices

Differences between Industrial and Consumer Devices

	Industrial machines	Consumer devices
Production volume	a few to many	a huge number
users	experts	General users
Cost	expensive	low
Maintenance	strongly managed	weakly managed
Environment	factories (almost stable)	factories
		User environments (diverse, open, and dynamic)

Characteristics of Consumer Devices

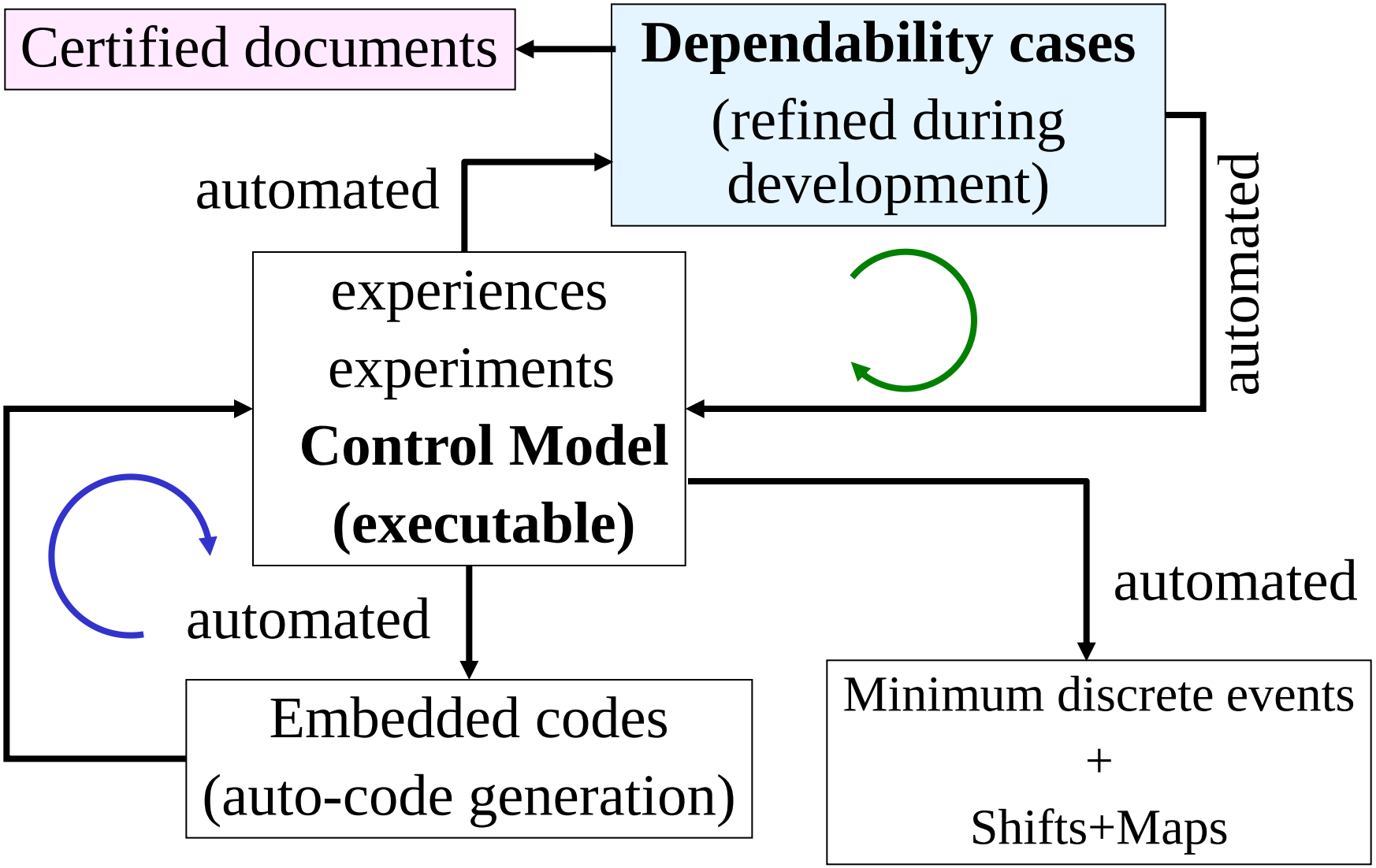


There are **accurate frequent interactions** with **high resolutions** between physical system and control software in **open, diverse, and dynamic** environment.

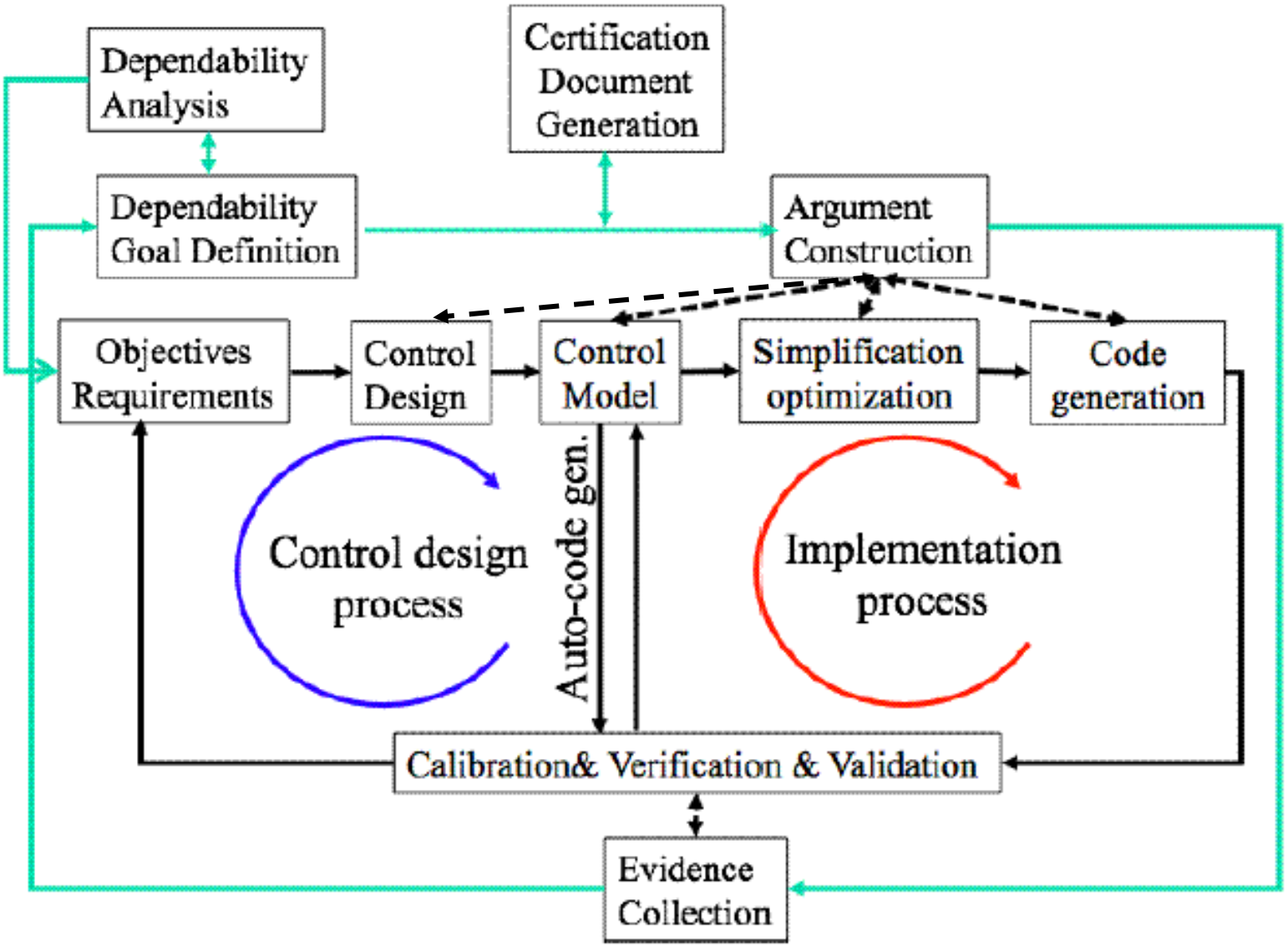
Important Aspects

1. Rapid iteration consistent with standard assuring dependability
2. Dynamical models to predict system behavior:
   - *Controller model*
   - *Controlled object model*
3. Physics in software:
   - *Software must reflect Physics of controlled object even if developers are not aware of the fact.*

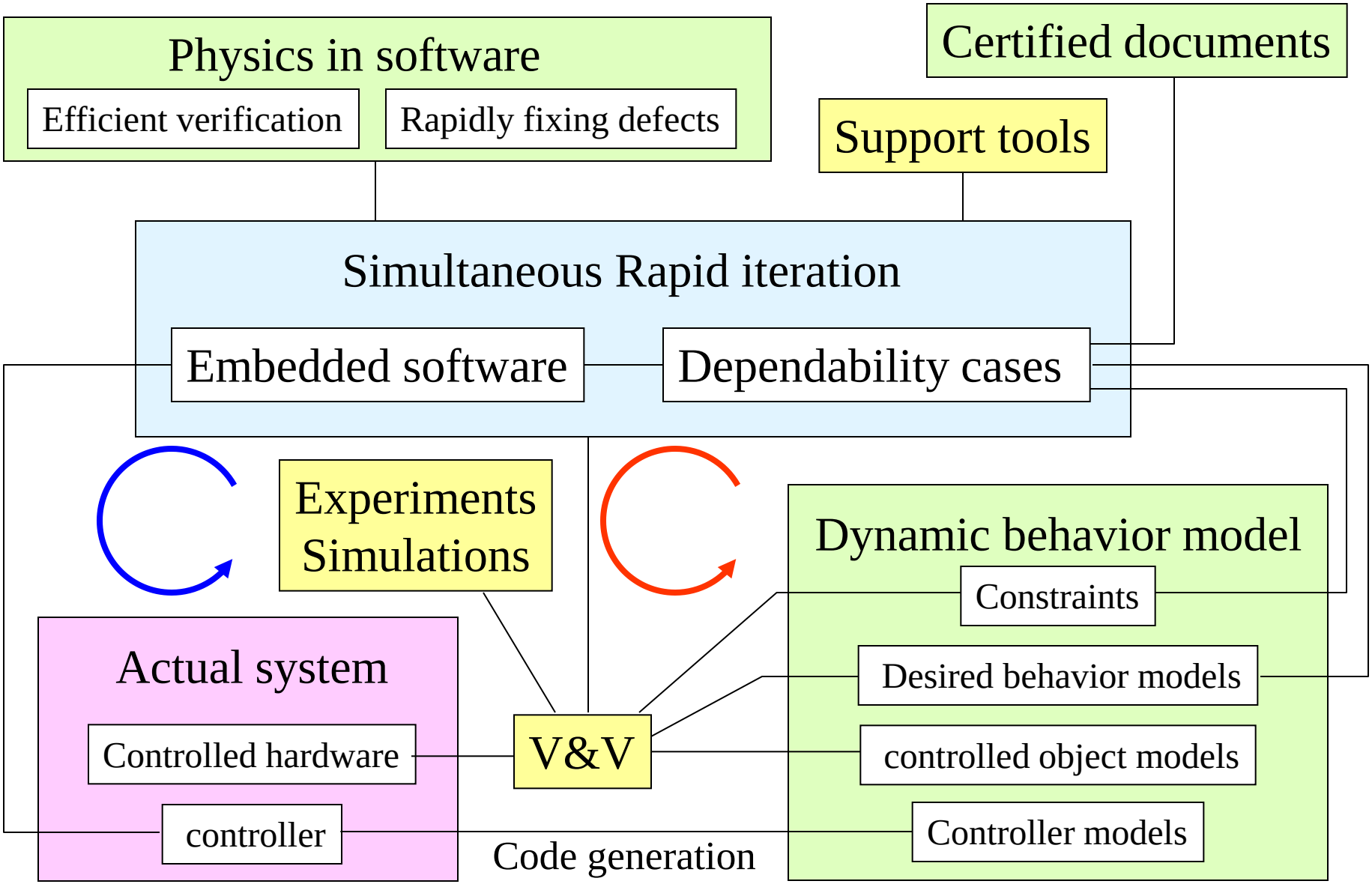
Proposed Process



Proposed Workflow



Scope of RFI → RFP



Standardization Process

1. RFI (Requirement For Information):

   The document or the process to gather useful information for an intended standardization.

2. RFP(Requirement For Proposal) :

   The document or the process to gather draft standards.

3. FTF(Finalizing Task Force):

   To establish the task force to finalize the standard.

4. ABV (Advisory Board Voting)

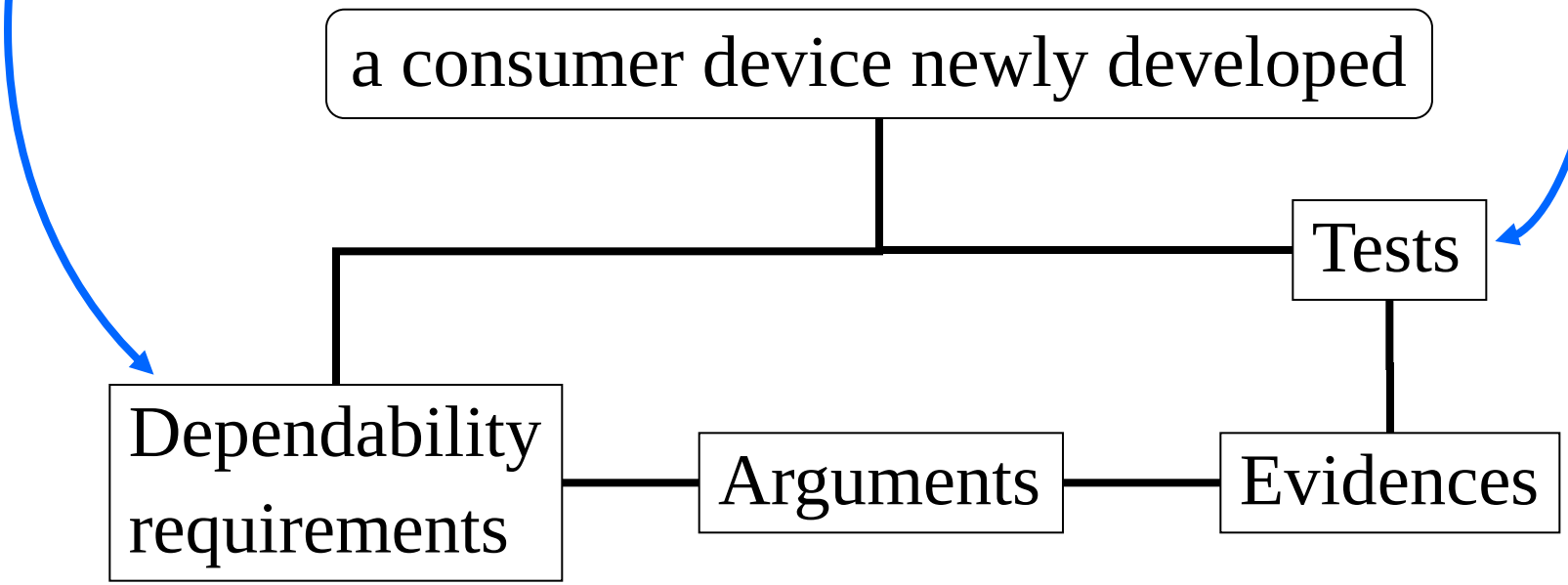
Contents

1. Review of RFI assuring dependability for consumer devices
2. Importance of prove in use
3. Responses for RIF
4. Moving toward RFP
5. Result of System Assurance Task Force (SysA)

Issue of Defining the Requirements

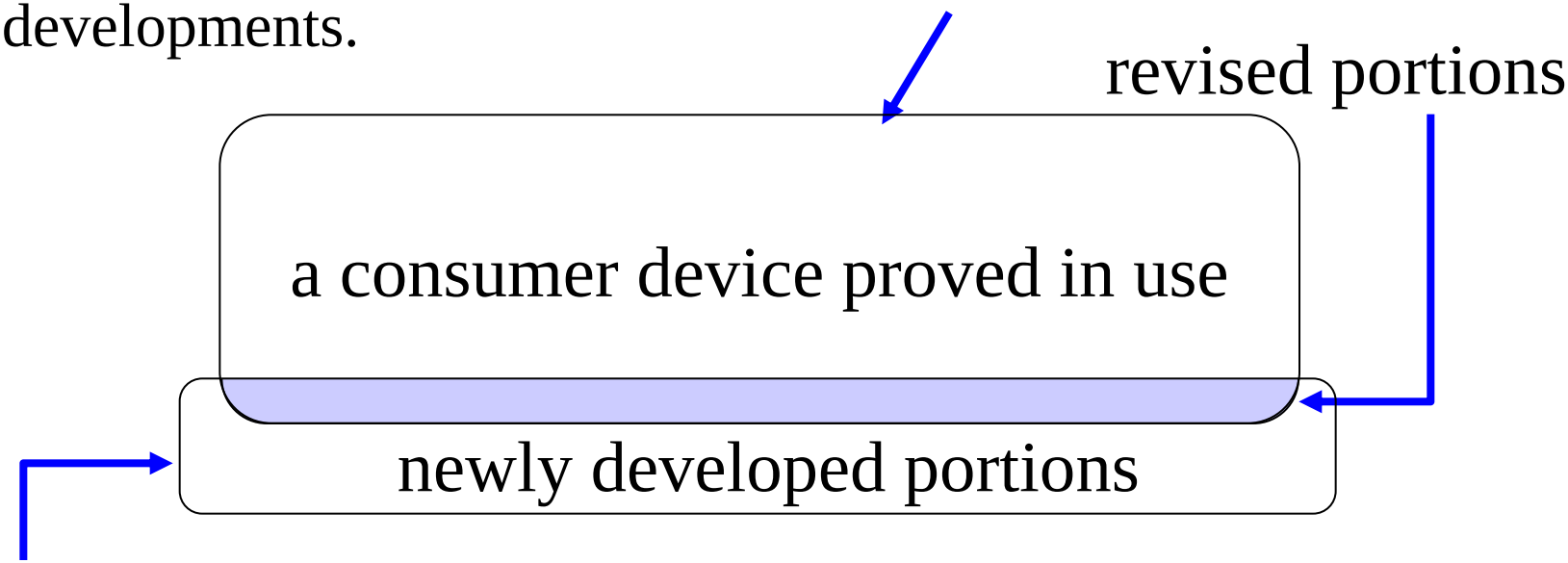
Issue: We have often encountered the difficulty to define all requirements that can be too many (NP hard problem).

We must perform an unreasonably huge number of the tests to get the evidences if all requirements must be proved during the development.



Fundamental Concept to Make Dependability Assurance Executable

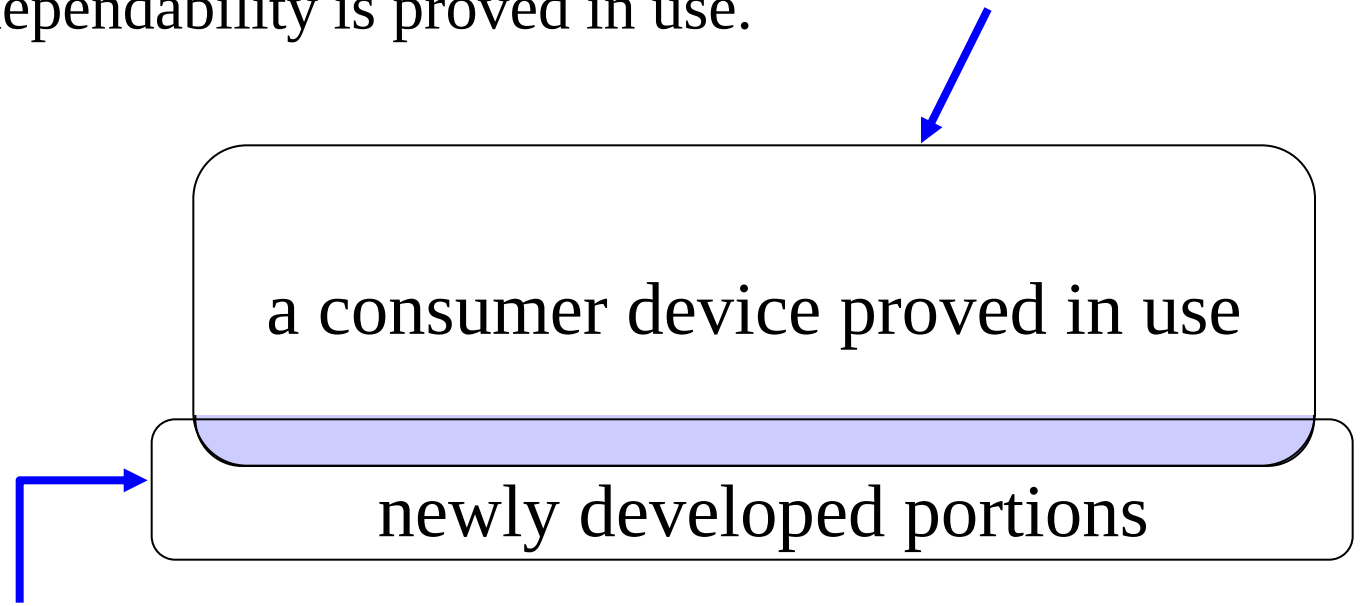
Many consumer devices are produced and used in various conditions for long time of which the evaluation coverage is extremely higher than the one reached by the tests during any developments.



The new product is sufficiently dependable if the newly revised portions are dependable. The concept can make the developments efficient and executable.

Proposed Approach

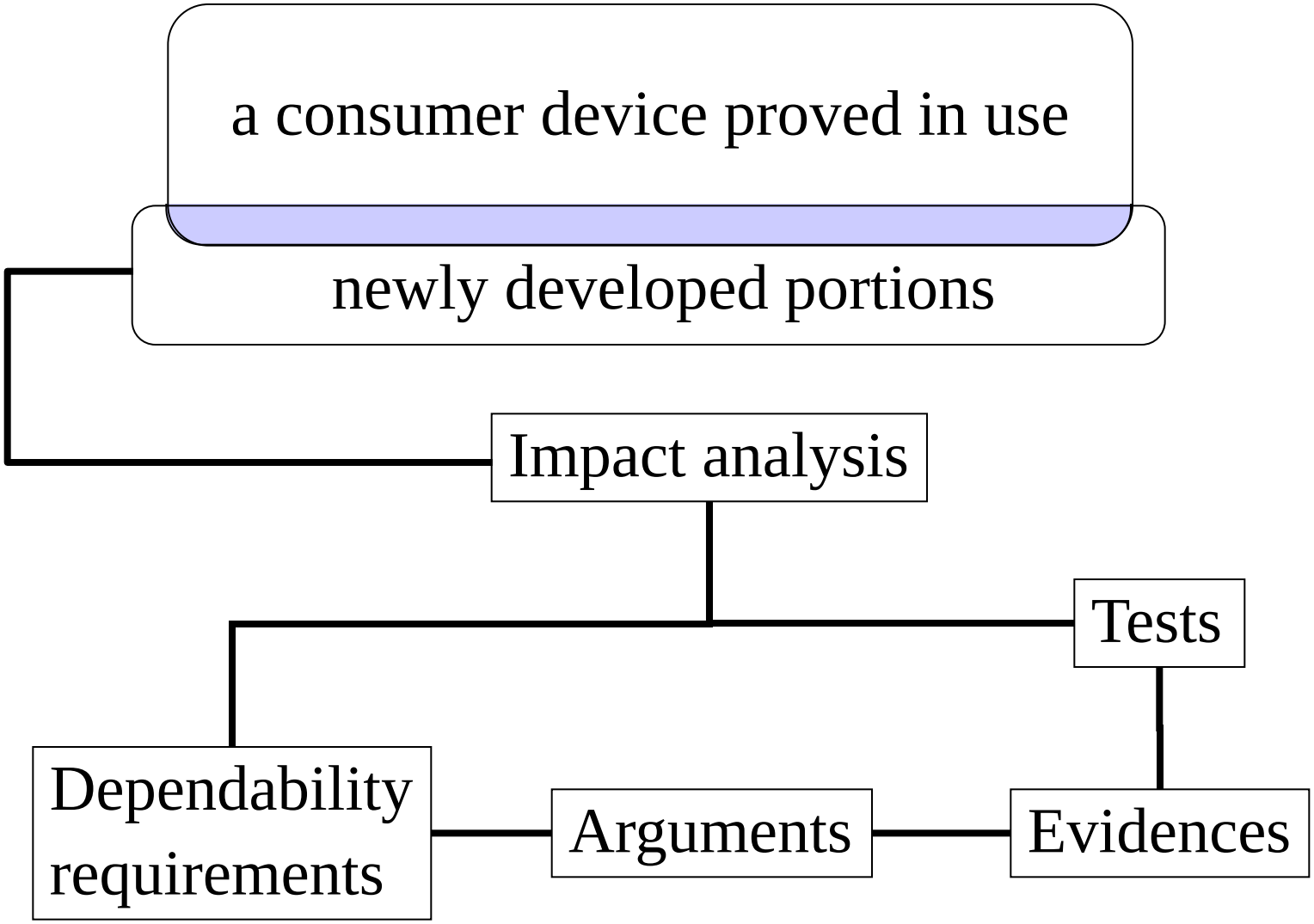
We don’t needs the evidence of this portions because the dependability is proved in use.



We focus on the portions different from the old product to develop the dependability cases.

The objective can be “Revised portion must not degrade the dependability of the base product.”.

Applying Dependability Cases



Contents

1. Review of RFI assuring dependability for consumer devices
2. Importance of prove in use
3. Responses for RIF
4. Moving toward RFP
5. Result of System Assurance Task Force (SysA)

Responses

1. Trusted Computing Group
2. Resilient Computing Lab., Department Science and Information, University of Florence
3. Dependable Operating Systems for Embedded Systems Aiming at Practical Applications (DEOS)

   Information and Communication Headquarters,

   Nagoya University
4. Toyota Motor Corporation

Trusted Computing Group (TCG)

TCG has created vendor-independent specifications for TPM (Trusted Platform Module) already implemented on 80% PC and TNC (Trusted Network Connect).

TPM and TNC enable to detect if a device or component within device are infected or improperly configured.

The EmSys (Embedded Systems Working Group) develops trust and security specifications for embedded computing platforms.

University of Florence

1. Outcome from ARTEMIS JU “CHESS” project
2. CHESS ML (CHESS Modeling Language) reuses subset of UML, SysML, and MARTE to address dependability concern.
3. CHESS ML supports different analysis methods representing the system at different abstraction level and having different objectives.

DEOS (Dependable Operating Systems)

1. GSN (Goal Structuring Notation) for Dependability Cases (D-Case)

2. DEOS process

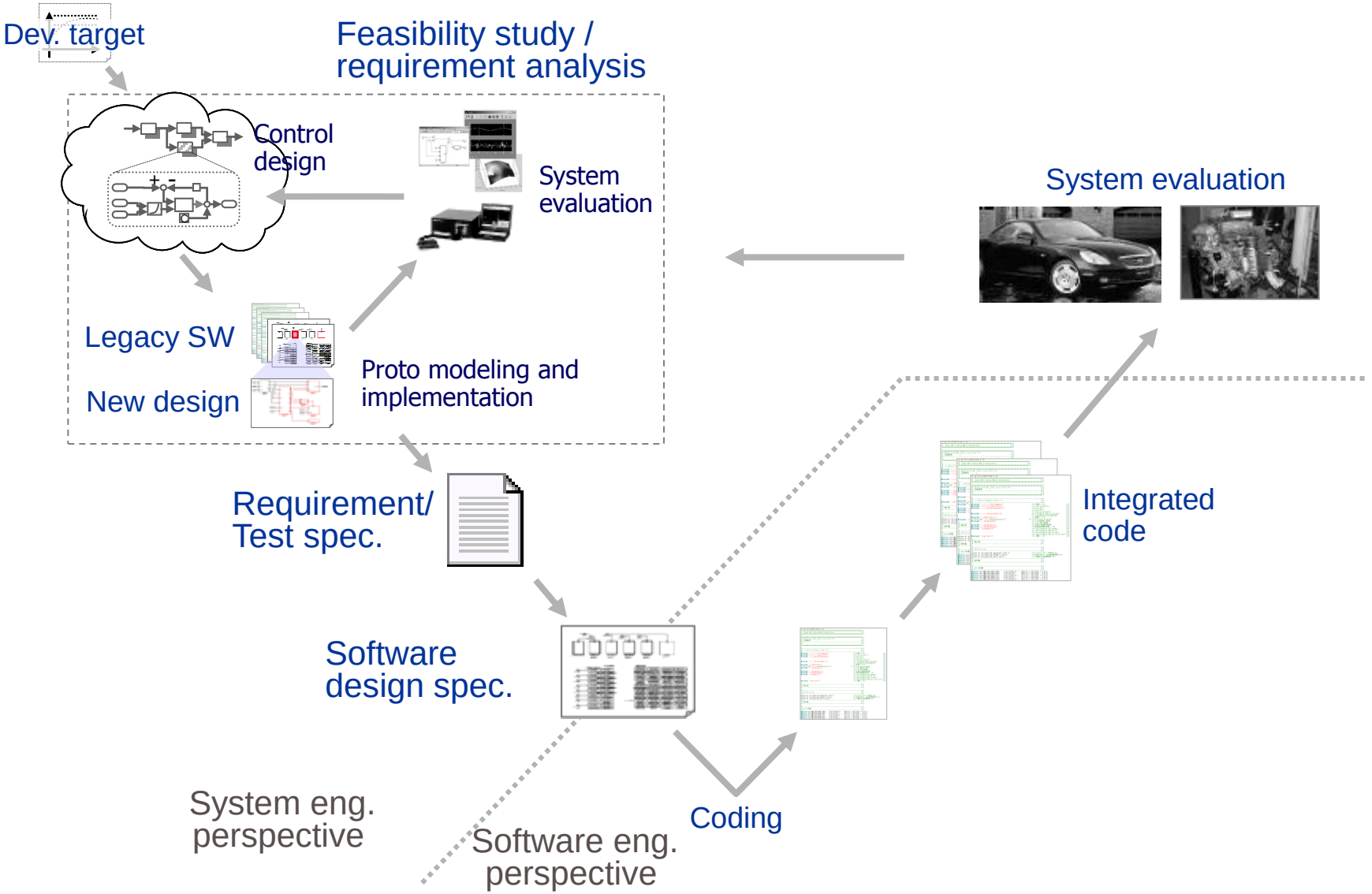
3. D-Case Editor

4. OMG standard such as ARM and SAEM

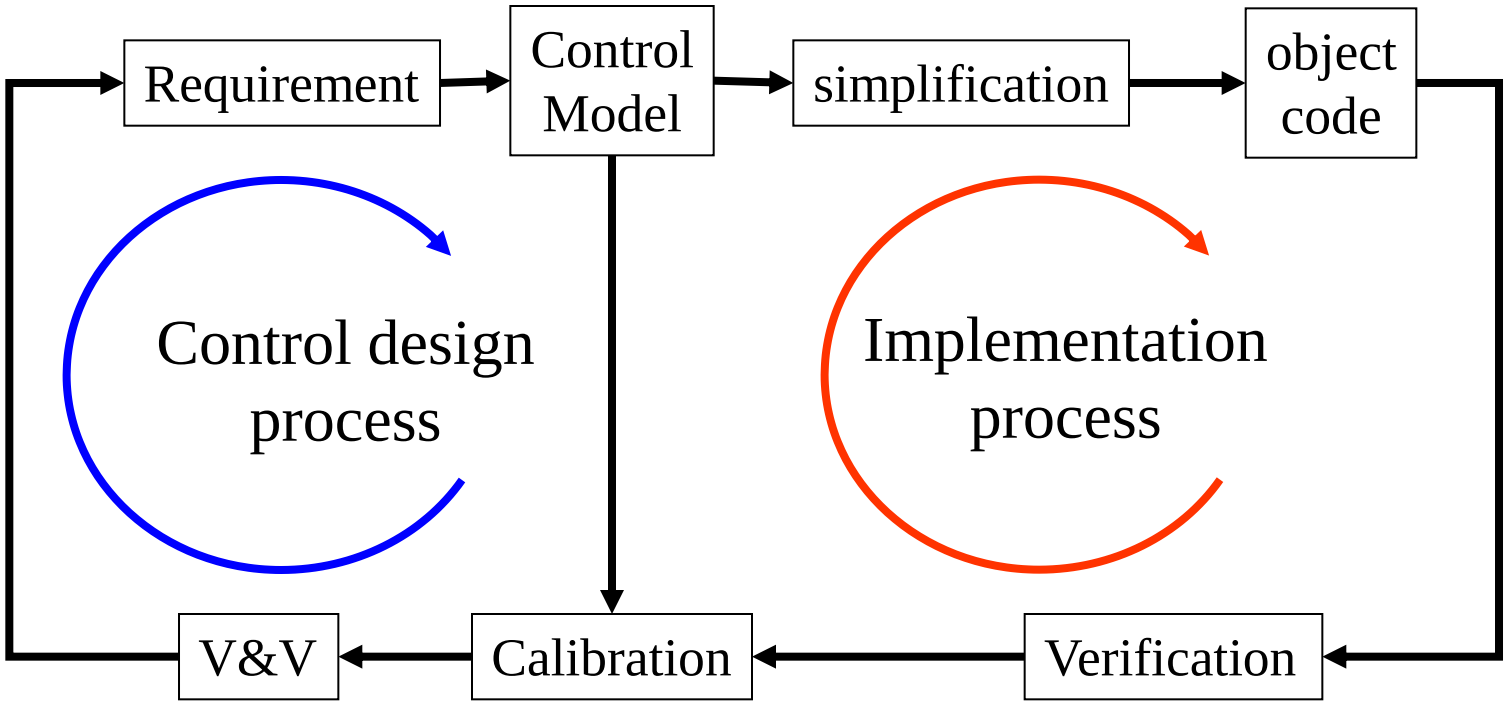
Toyota

1. Design-based validation
2. Property Proving on Snapshots
3. Snapshot Covering Test
4. Live Dataflow Identification

- Incremental and iterative development



MBD workflow in RFI



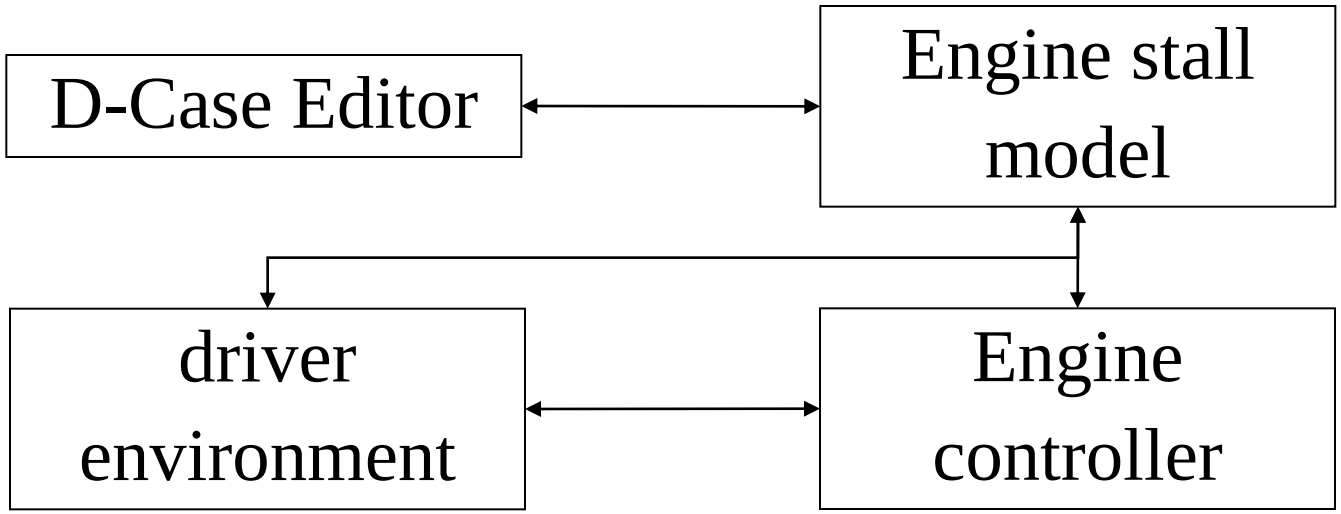
Contents

1. Review of RFI assuring dependability for consumer devices
2. Importance of prove in use
3. Responses for RIF
4. Moving toward RFP
5. Result of System Assurance Task Force (SysA)

Proposed Schedule

1. In the next SysA in September, we would like to show a possible process assuring dependability of consumer devices with demonstration of simple model simulating engine stalls.
2. We would like to submit a draft RFP to SysA in December according to the reflections from the responses.
3. Hopefully, we would like to issue RFP in the first sysA in March, 2013.

Model for Demonstration



1. Components are integrated
2. To visualize development process and data exchanges
3. To visualize required tool chain

Possible Items of Proposed Standard

1. Simultaneous development process of embedded software and dependability cases (D-case)
   - ① *Theoretical basis of "prove in use"*
   - ② *Derivational/clone development*
   - ③ *Iterative process of embedded software and D-case.*
2. Dynamic behavior model
   - ① *Controlled object model*
   - ② *Controller model*
3. Calibration process
   - ① *Theoretical back ground of calibration maps*

Collaboration

- DEOS Process, MBD process, Design-based validation
- Dynamic Behavior models of controlled object and controller modes
- D-Case Editor
- OMG standard such as ARM and SAEM
- CHESS ML
- Development platform with TPM and TNC
- Meta-model of ISO26262

Contents

1. Review of RFI assuring dependability for consumer devices
2. Importance of prove in use
3. Responses for RIF
4. Moving toward RFP
5. Result of System Assurance Task Force (SysA)

Result of SysA

SysA requires us to submit a white paper including

1. Scope
2. Road map
3. Background

by September, 2012.

We would like to put this activity forward with you!

- enhancement of “prove in use”
- real advantages for users and automotive industry
- advances of safety, reliability and sequrity