Challenges to Improve the Confidence in Cyber-Physical Systems

Tetsuya TOHDO
ePF Advanced R&D Dept.
DENSO CORPORATION
<table>
<thead>
<tr>
<th><strong>Established</strong></th>
<th><strong>December 16, 1949</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capital</strong></td>
<td>187.4 billion yen (US$1.6 billion)</td>
</tr>
<tr>
<td><strong>Revenue</strong></td>
<td>4,524.5 billion yen (US$40.2 billion)</td>
</tr>
<tr>
<td><strong>Operating Profit</strong></td>
<td>315.7 billion yen (US$ 2.8 billion)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Employees</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consolidated basis</strong></td>
<td>151,775</td>
</tr>
<tr>
<td><strong>Non-consolidated basis</strong></td>
<td>38,490</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Consolidated Subsidiaries</strong></th>
<th>188</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Japan 62, North America 28, Europe 34, Asia 58, South America/Others 6)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Affiliates under the Equity Method</strong></th>
<th>36</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Japan 13, North America 4, Europe 4, Asia 13, South America/Others 2)</td>
<td></td>
</tr>
</tbody>
</table>

Notes:
U.S.dollar amounts have been translated, for convenience only, at the rate of 112.68 yen = US$1, the approximate exchange rate prevailing on March 31, 2016. Billion is used in the American sense of one thousand million.
Products

Environment
Hybrid and electric vehicle components, Products for fuel cell vehicles, gasoline engine management system, diesel engine management system, starter, alternator, radiator, etc.

Comfort & Convenience
Car air-conditioning system, air conditioner for buses, air purifier,

Car navigation system, electronic toll collection system (ETC), remote security system, remote touch controller, smart key, advanced vehicle operation system (AVOS), etc.

Safety
Sensing technologies for driving assist systems, actuator & computer for antilock brake system (ABS) / electronic stability control (ESC), adaptive front-lighting system (AFS), airbag sensors & electronic control units, periphery monitoring system, instrument cluster, rain sensor for automatic windshield wiper, etc.

Non-Automotive Fields
Home Appliances, Heating and Cooling Equipment, Auto ID Data Capture Devices, Factory Automation Products
Outline

- Introduction
- MBD (Model-Based Development)
- Functional Safety
- Advanced Topics
- Testing
- Summary / Conclusion
Introduction
Automotive Systems

- **Electronics**
  - add new features
  - improve control performance (environment, safety)
As Cyber-Physical Systems

- **Automotive E/E Systems**

[Diagram showing Driving Context, Physical Phenomena, and Human Operation]
As Cyber-Physical Systems

- Physical
  physics (chemical, ...)

- Cyber
  computation
Embedded Software

- **Complex system behavior**
  Need confidence in design

- **Technologies**
  Simulation
  Formal Verification
  Test Vector Generation

- **Experience**
  Test oracle is hard
Embedded Software

- Cyber-Physical
  Functionality of SW designed at system-level
  Various disciplines relate to each other

- This talk
  Design, analysis and testing
  System and software level
MBD

Model-based Development
Originally, model-based (control) design

- Plant model
- Controller model

Physical constraints

Now, use of simulation technologies
  → Model-based development
Vehicle Energy Flow

Coolant circuit

HVAC

Batt

Electrical component

Transmission

Engine

Electrical circuit
Simulation: Example

- Domain → specific simulation
- Tool Integration

![Diagram showing various components and simulation integration](image)
Simulation : Example

- Result

![Graphs showing experimental and simulation results for various parameters such as vehicle speed, engine revolution, fuel injection, coolant temperature, and cabin temperature over time.](Graph.png)

- Simulation : Example

  - Result

  $\frac{14}{58}$
MBD Technologies

Plant

Controller
Simulation

- Flexible
Rapid Prototyping

- Precise dynamics
HIL (Hardware in the Loop) simulation

- Reduce space and time
- Extreme condition
MBD Contribution

- Efficient development
  Replace prototype (vehicle …) with simulation

- Improve performance (quality of control)
  Flexible setting including extreme conditions
MBD Side Effect

- **Demand**
  - Precision plant simulation
  - Performance designed control

- **Iterative improvement**
  - Models → complex and detailed

- **Confusing role**
  - requirement? implementation?
  - → Need to keep concepts (requirements)
Functional Safety
Functional Safety: Scope

- Safety of E/E systems

  Vehicle: safety critical  various safety (by use case)

Collision safety  Functional safety
Functional Safety: Background

- **In-vehicle network**
  E/E subsystems connected (2000~)

- **Functional safety for automotive (research)**
  Apply IEC61508 (2000~)
  Advanced development methods

- **ISO26262**
  WG (2005~) → published 2011
Safety

- **State**
  without cause of hazard, ideally

- **Social acceptance**
  ISO/IEC Guide 51
tolerable (acceptable) risk

\[
\text{risk} \triangleq \sum \text{damage} \times \text{probability}
\]
What is the safest car?

→ Safety is prior to functionalities
Safety of E/E systems (ISO26262-1:2011)

absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems

Example

Context: Driving (highway)
Hazard: Air bag (inflating by failure)
Failures (Faults)

- Random hardware faults
- Systematic failures

Today’s topic → Software
Focus on “systematic failures” only
Safety Design

- **Concept Phase**
  - Vehicle level use case
  - Hazard
  - Functional Safety Concept

- **Design Phase**
  - Safety requirements
  - Architectural Assumption

  Hierarchical Activities
  - Decompose requirements
  - Allocate requirements to sub components
  - Safety Analysis
Example

- **Safety Concept**
  
  use redundancy to detect failure
Software Safety Requirement

- **Functionalities**
  - allocated to Software

  e.g.
  “Complete safety reaction within specified time”
Software Safety Analysis

- Consider Failure
- Analyze Influence
  - confirm safety
  - add safety mechanism, if necessary
Software Safety Analysis

- **Div by Zero**

  - add guard
    - covered by design rule
    - static verification

**SA : Data Retrieval**

**SB : Data Retrieval**

**SensorA**

**Signal A**

**Signal B**

**F : Intended Function**

**Detection**

**Safety Reaction**

**WD Timer**

**SensorB**

**Output Device**

**Safety Reaction (external HW)**

**RTOS**

- Div by Zero
  - add guard
    - covered by design rule
    - static verification

(CERTIFIED TIVY)
Software Safety Analysis

- Round Error Accumulation
  → already covered
  • redundancy with diverse signals

- Signal A
- Signal B
- F: Intended Function
- Detection
- Safety Reaction
- Hardware
- Sensor A
- Sensor B
- WD Timer
- Output Device
- SA: Data Retrieval
- SB: Data Retrieval

(Calibration HW)
Software Safety Analysis

SA : Data Retrieval

F : Intended Function

SB : Data Retrieval

Detection

Safety Reaction

O : RTOS

Signal A

Signal B

Slipped Triggers

(deadline miss)

(External HW)
Software Safety Analysis

- New requirements (new components)

Signal A

F: Intended Function

Detection ➔ Safety Reaction

M: Runtime Monitor

O: RTOS

SensorA ➔ WD Timer ➔ SensorB ➔ Safety Reaction (external HW) ➔ Output Device

SA: Data Retrieval ➔ F: Intended Function ➔ Detection ➔ Safety Reaction

Hardware

Software
Lessons learned from Functional Safety

- **Design** → **Hierarchical Activities**
  - Decomposition
  - Allocate requirements

- **Component may fail**
  - Not trust too much

- **Analysis at architectural abstraction**
  → **systematic mitigation using both**
  - Runtime mechanisms
  - Design time measures
Advanced Technology

- **ADAS** Advanced Driving Assistance System
- **AD** Automated Driving

www.denso.com

Test on public road & Demonstration driving (2014-)
ADAS / AD Architecture

- Actuator controls
- Sensor fusions
- Services (use cases)
- Human factors

Sensor Manager
- MMW RADAR
- LIDAR
- Camera
- Ultra sonic
- Wireless com.
- Driver Monitor

Service
- Adaptive Cruise Control
- Collision Mitigation
- Prevent misacceleration
- Auto Parking
- Auto Lighting Control
- Lane Departure Warning
- Collision Warning
- ...

Safety Manager
- Vehicle Motion Control

ECU
- Engine
- ESC
- EPS
- Light Control

HMI Manager
- Instrument Cluster
- Center Display

Driver
- Engine
- Brake
- Steering
- Light

Driver Monitor

This information is the exclusive property of DENSO CORPORATION. Without their consent, it may not be reproduced or given to third parties.
Identifying Objects

Performance required depending on use case
## Level of Automation

<table>
<thead>
<tr>
<th>SAE Level</th>
<th>Control</th>
<th>Monitor</th>
<th>Recover</th>
<th>Usecase</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Driving</td>
<td>Driver</td>
<td>Driver</td>
<td>Driver</td>
</tr>
<tr>
<td></td>
<td>Automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td>Driver and System</td>
<td>Driver</td>
<td>Driver</td>
</tr>
<tr>
<td>2</td>
<td>Partial Driving</td>
<td>System</td>
<td>Driver</td>
<td>Driver</td>
</tr>
<tr>
<td></td>
<td>Automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Conditional</td>
<td>System</td>
<td>System</td>
<td>Fallback-ready user</td>
</tr>
<tr>
<td></td>
<td>Driving Automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>High Driving</td>
<td>System</td>
<td>System</td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Full Driving</td>
<td>System</td>
<td>System</td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Automation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Source: SAE J3016™ Sep2016 (simplified)*
Functionalities depend on contexts
same sensors, same actuators, different use-cases

e.g. highway driving / parking
Advanced Technologies: Challenge

Complex Environment

- Various Contexts
- Human Factors
Testing
What is testing?

- Input stimuli, and

- Observe
What is testing?

- Input stimuli and observe
- Used for various objectives
Testing: Usage

- Input stimuli and observe
- Used for Prototyping Advanced Dev.
Testing : Usage

- Input stimuli and observe

- Used for

Verifying design
Testing: Usage

- Input stimuli and observe
- Used for Qualifying Products
Testing : Usage

- **Validation**
  Correct Requirements?

- **Verification**
  Correct Product?
Quality of Requirements

- Be verifiable
- Should specify
  “What to achieve” for the component

- In reality, often “how to calculate”
Test Oracle

- **Selection**

  Design space of test case

  with hypothesis

- **Observation**

  Distinguish **correct** and **bad**

My View

- Selection Coverage (incl. Assumptions)

- Observation Requirements (Correctness)
Vision

Correctness

Requirement-based

Design, Analysis,

Testing

Combination

Coverage

No strategy
Summary

- Automotive E/E systems
  Cyber-Physical Systems

- Evolution
  Enabled by Simulation technologies (MBD)

- Safety
  Managing complexity by architectural design

- Advanced challenge
  Need to overcome complex environment

- Testing → provide confidence
  by integration with design and analysis
Cyber-Physical Systems

- Embedded software needs safety and reliability
- Software brings new values and services
  - Various disciplines, related
- Expertise will contribute in the industrial context, combined with other knowledge

Crafting the Core