Why We Need Something New in the Automotive Industry

Dr. Qi Van Eikema Hommes

April 19, 2012

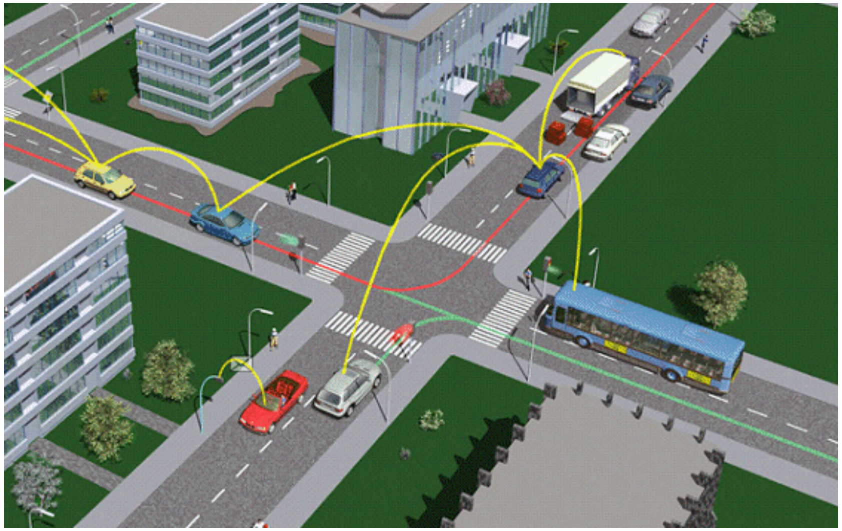
1896

Henry Ford in his first car, the Quadricycle, built in 1896

Let The Robot Drive

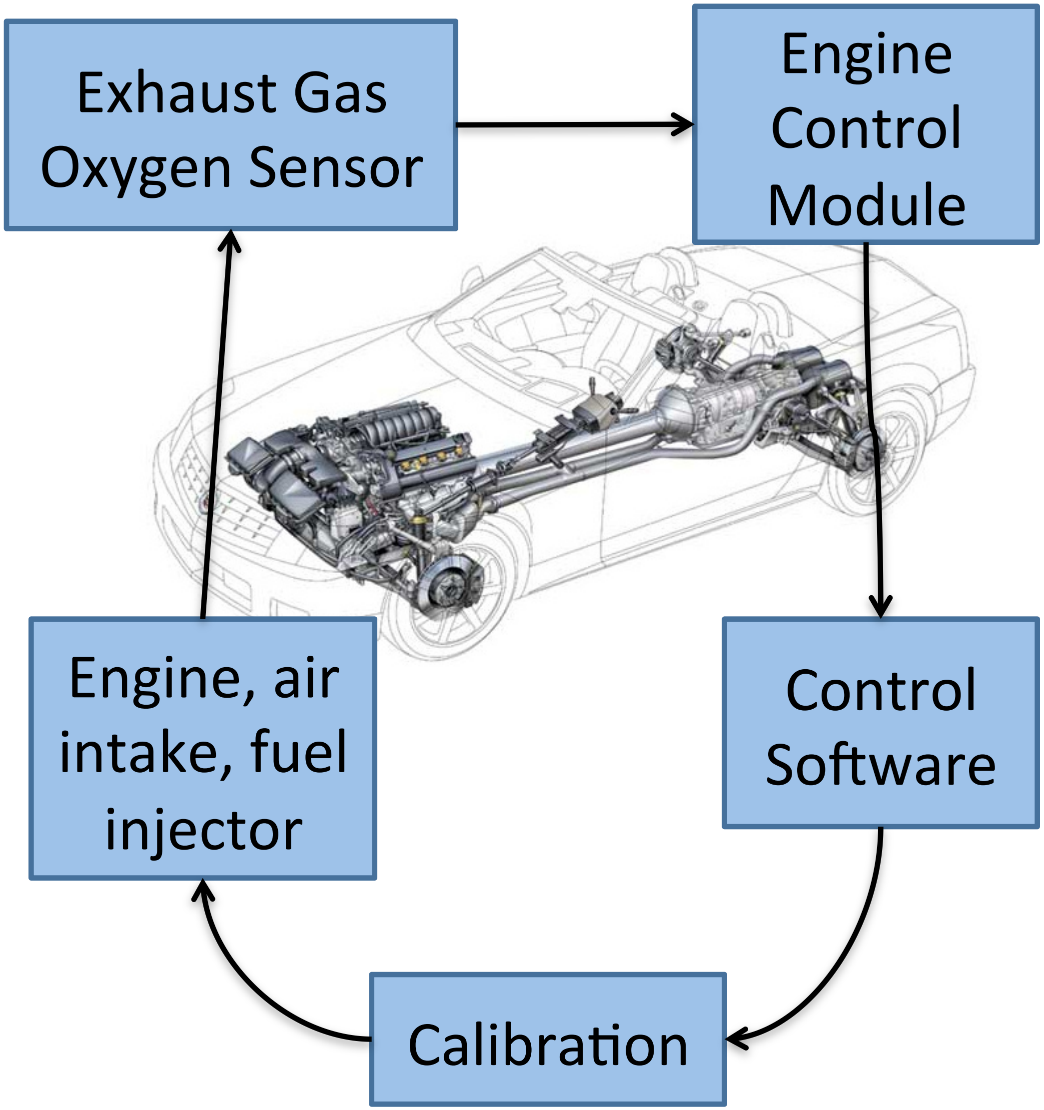
Wired, Feb 2012, http://www.wired.com/magazine/2012/01/ff_autonomouscars/all/1

Automotive Systems Today and Tomorrow



- **Cyber Physical Systems**- complex embedded devices networked to control physical hardware components.
- Software intensive.
- Automating many human tasks.
- The development teams are multidisciplinary and globally distributed.

Quality Problem With no Component Failure



- Trouble-Not-Identified Engine Control Module warranty problem.
- No component failure was found.
- Insufficient resource to conduct exhaustive bottom-up testing, after the product was already released to market.
- Many such quality problems are never resolved.

Toyota Unintended Acceleration

The Detroit News www.detnews.com

April 6, 2010 http://detnews.com/article/20100406/AUTO01/4060371

Toyota faces $16.4M fine for hiding safety defect

Proposed penalty is largest ever sought by NHTSA officials

DAVID SHEPARDSON
Detroit News Washington Bureau

Washington -- Federal safety regulators are seeking to fine Toyota Motor Corp. $16.4 million -- the largest ever penalty against an automaker -- for failing to disclose problems with sticky accelerator pedals in a timely manner.

EARNINGS | February 9, 2011

U.S. Blames Drivers, Not Toyota

Investigators Clear Car Electronics for Instances of Unintend Contributed

Article | Video | Interactive Graphics | Stock

SUBSCRIBER CONTENT PREVIEW

FOR FULL ACCESS: LOG IN OR SUBSCRIBE NOW - GET 8 WEEKS FREE

BY JOSH MITCHELL, MIKE RAMSEY AND CHESTER DAWSON

Federal highway safety officials on Tuesday absolved the elec Corp. vehicles for unintended acceleration, and said driver err the incidents.

Wall Street Journal

March 30, 2010 http://detnews.com/article/20100330/AUTO01/3300329

NASA to help probe unintended auto acceleration

DAVID SHEPARDSON
Detroit News Washington Bureau

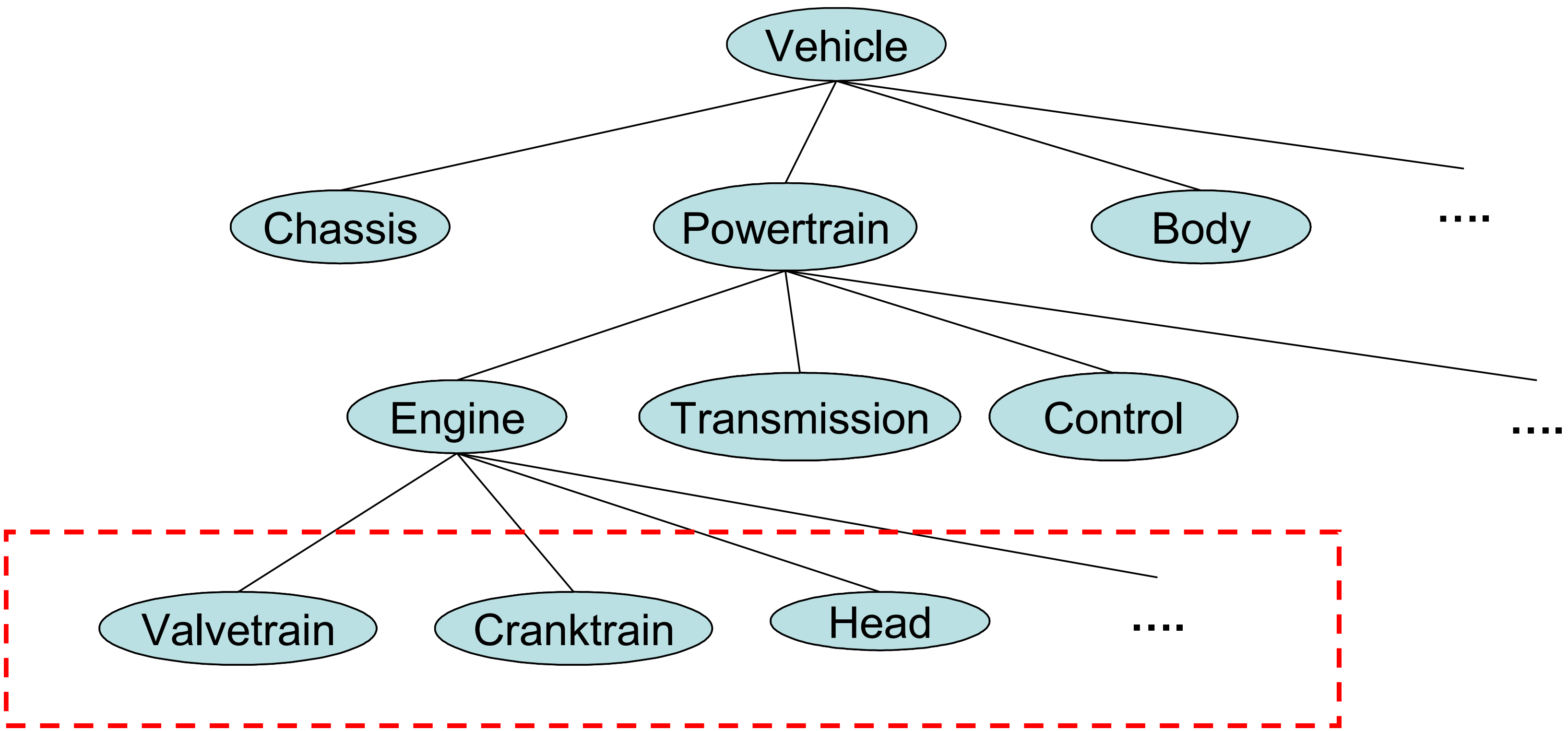
Washington -- The U.S. Transportation Department will launch two major investigations to discover whether vehicle electronics or electromagnetic interference are to blame for unintended vehicle acceleration incidents.

Typical Decomposition Scheme

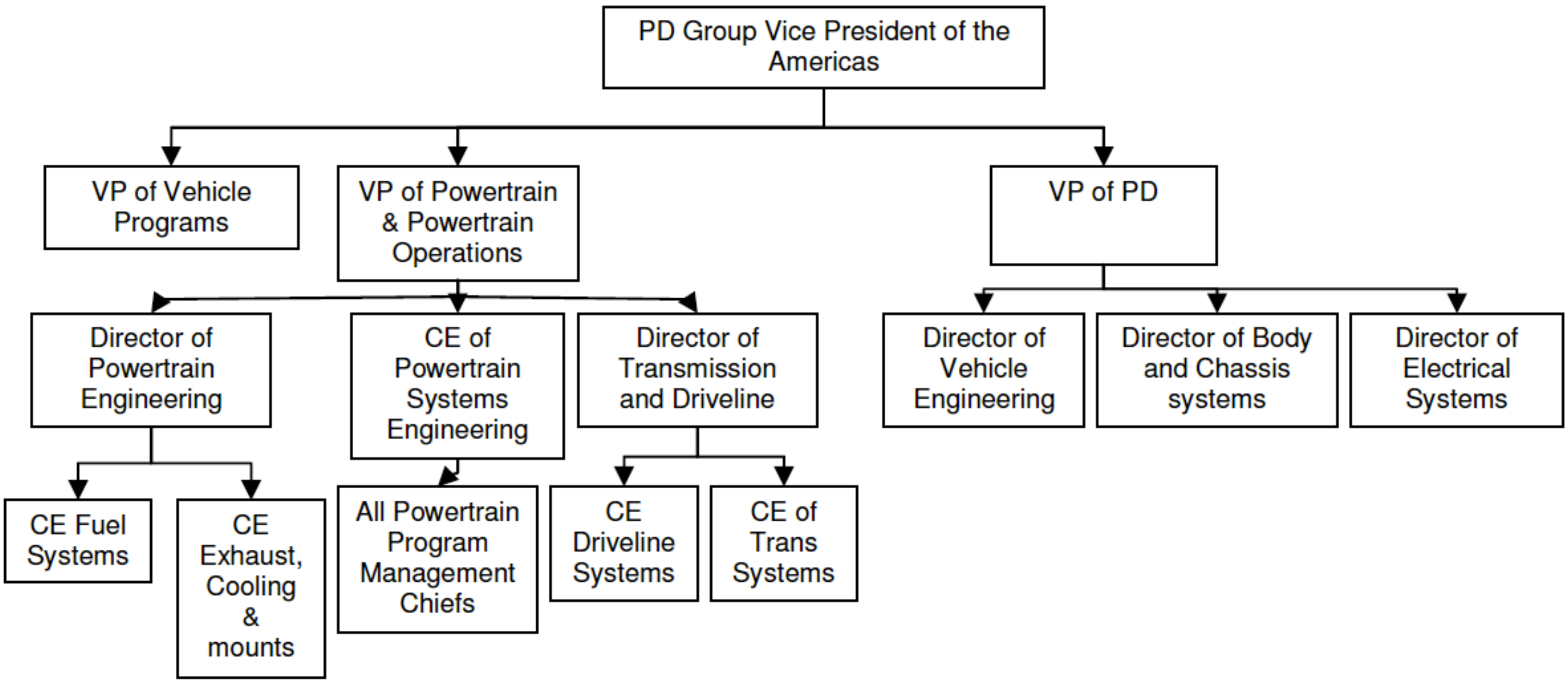
- **Physical**: usually stated as systems, subsystems, subassemblies, parts
  - Car systems and subsystems include seats, engine, suspension, steering
- **Organizational**: Usually stated as divisions, departments, groups, etc.
  - Powertrain department, Research and Development division, etc.
- **Process:** usually stated as phases of the product development process.
  - Concept development, detailed design, etc.

Example of a Vehicle Engineering

Physical Decomposition



Organization Decomposition



Adapted from: Michelle Sackas, *A Systems Engineering Approach to Improve Vehicle NVH Attribute Management*. MIT SDM Thesis, 2008.

Process Decomposition

1. Concept

Description of Activities:

- Idea Generation:
  - Requests
  - Customer Pain
  - Market Studies
  - Legislation
  - Competitors

Key Deliverables:

Product Concept Doc.

2. Research

Description of Activities:

- Assess Market:
  - Segments & Size
  - Growth Potential
  - Customer Needs
  - Legal Issues
  - Competition

Key Deliverables:

Market Research Report

Market Req. Document

Product Definition Statement

3. Analysis

Description of Activities:

- Business Analysis:
  - Cost/Benefit
  - Resources Required
  - Capital Expenses
  - Profitability/Margin
  - Anticipated Sales

Key Deliverables:

Business Case

Profitability Analysis

Product Req. Document

4. Develop

Description of Activities:

- Product Development:
  - Technical Specs
  - Prototyping
  - Trial Production
  - Testing & QA
  - Test Market Selling

Key Deliverables:

Product Dev. Schedule

Product Testing Report

Test Market Sales Report

5. Launch

Description of Activities:

- Go To Market:
  - Marketing Plan
  - Sales Training
  - Distribution Plan
  - Collateral Design
  - Set Launch Date

Key Deliverables:

Product Launch Plan

Product Launch Budget

Product ROI Forecast

Target Launch Date Set

Checkpoint #1

Description of Activities:

- Review Deliverables

Decisions:

Checkpoint #2

Description of Activities:

- Review Deliverables

Decisions:

Checkpoint #3

Description of Activities:

- Review Deliverables

Decisions:

Checkpoint #4

Description of Activities:

- Review Deliverables

Decisions:

Checkpoint #5

Description of Activities:

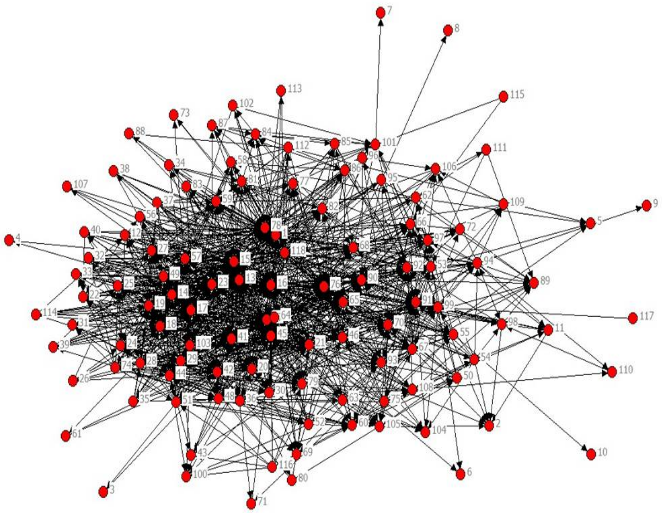
- Review Deliverables

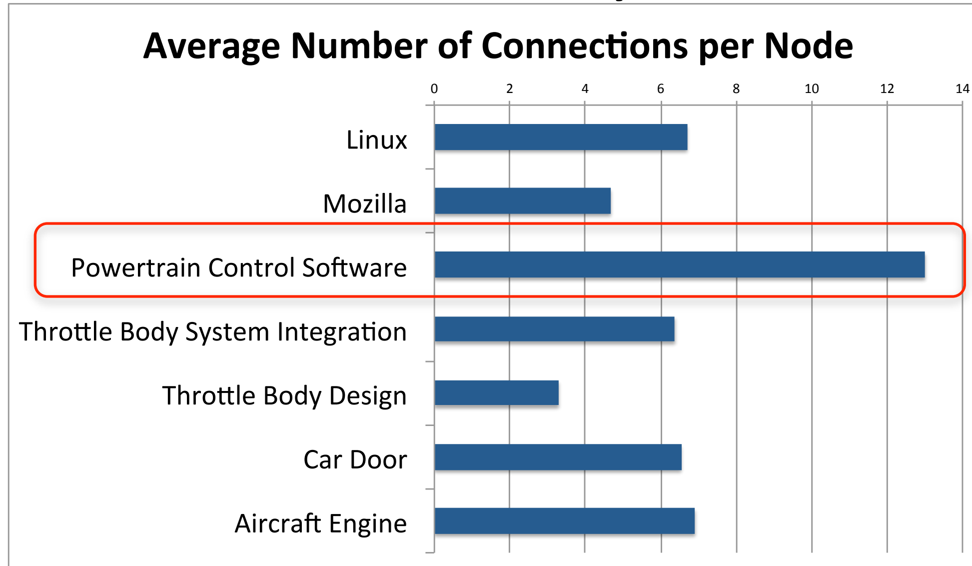
Decisions:

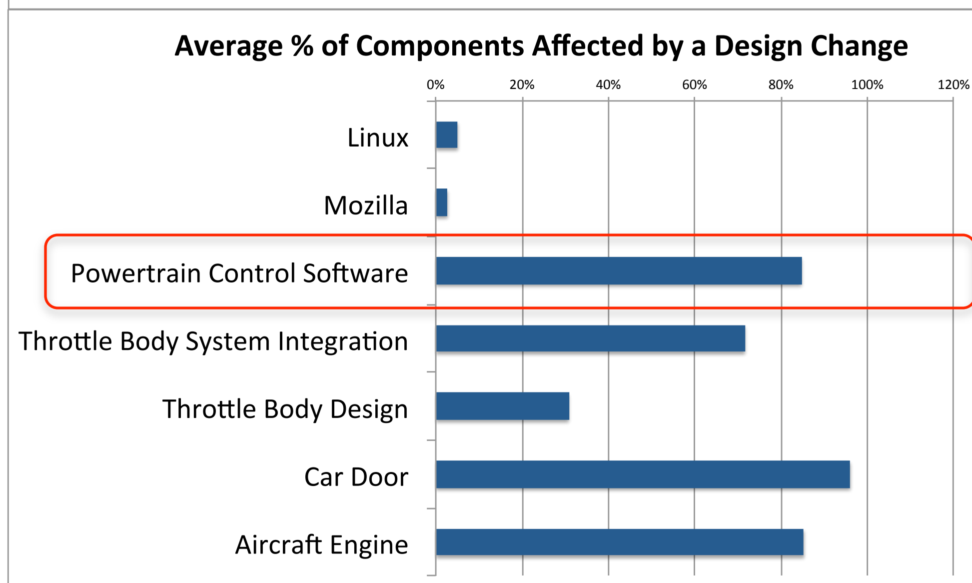
The Effect of Decomposition

- Quality and safety = component failure prevention
  - Failure: Not performing intended function
- Quality and Safety Engineering = Reliability Engineering
- Component failures are random hardware failures
  - Not useful for complex software system
  - Not useful for social systems
- Bottom-up hazard analysis based on linear chain-of-events model, ignoring systemic factors.
- The reality: many unresolved quality problems.

An Example of System Interactive Complexity: The Powertrain Control Software System



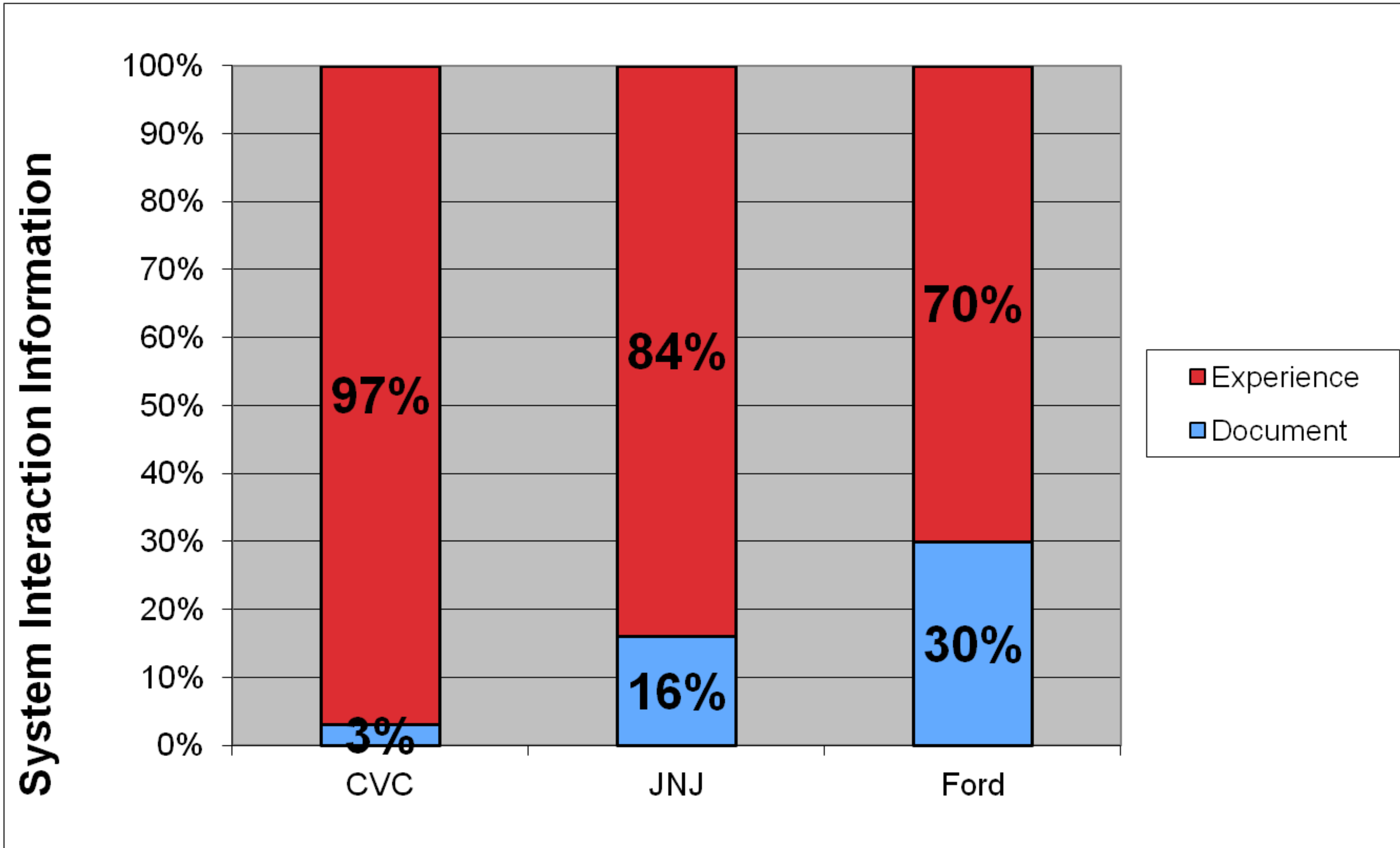




- 1 production-level software
- 117 software modules (red dots)
- 1423 interactions (black lines)
- 39 such production software releases per year
- <2 weeks per release

Hommes, DETC2008-DTM-49140

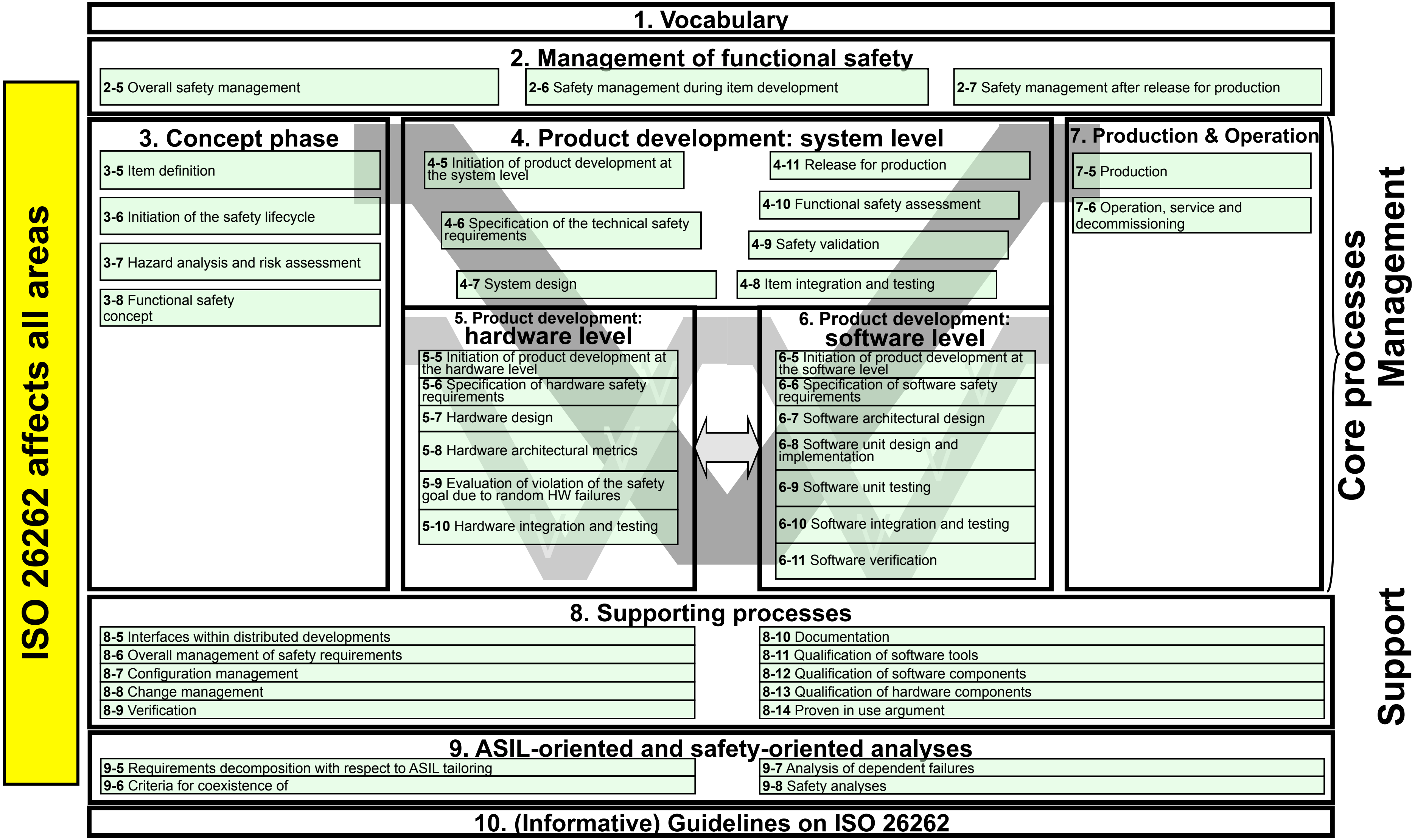
We Rely Heavily on Experts' Tacit Knowledge to Handle System Interactions and Integration



ISO 26262 Functional Safety for Road Vehicle

- The first comprehensive standard that addresses safety related automotive systems comprised of electrical, electronic, and software elements that provide safety-related functions.
- Adaptation of IEC 61508 to road vehicles
- Influenced by ISO 16949 Quality Management System

General Structure of ISO 26262



Source: ISO 26262

Strengths

- Emphasizing safety management and safety culture
- Prescribes a systems engineering process
- Departure from safety as an after-thought:
  - IEC 61508: safety function
  - ISO 26262: provides the framework and vocabulary for hazard elimination in the first place
    - Systems engineering framework
    - Safety measure vs. safety mechanisms

Suggestions for Improvements

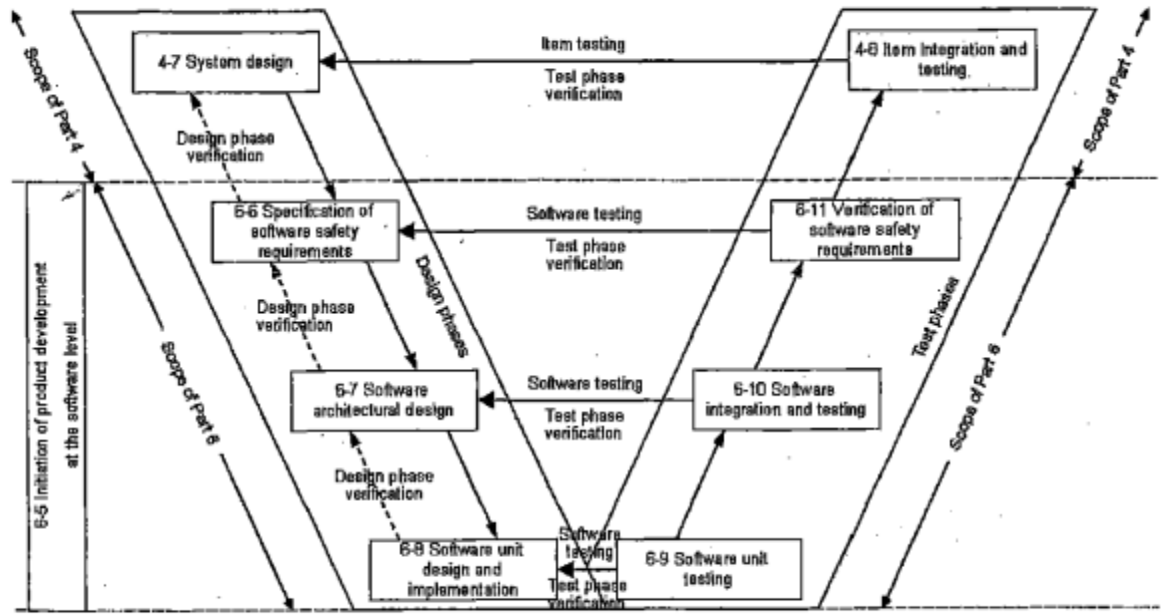
- Safety measure is not clearly explained in the document, while Safety Mechanism is explained in detail throughout the document.
- The standard may want to add a section in Part 1 to further clarify the departure from IEC 61508's design philosophy.

Reliability Engineering Methods in ISO 26262

- **Hardware Architecture Metrics--**Based on random failure of components.
- **Failure Modes and Effects Analysis (FMEA)**
- **Fault Tree Analysis (FTA)**
- **Safety Case Approach**
  - Confirmation bias
  - Independent reviewers are less familiar with the design
  - The use of Quantitative Risk Assessment
- **Investigate the effectiveness of STPA and how to integrate it with the standards to provide higher safety assurance.**

Software Safety

- Follows software system engineering process
- Promotes good software architecture practices
- Best practices in software design
- Addresses hardware failure
- On Par with other software safety standards such as DO-178



Comments:

- Unlike hardware, software does not fail.
- Software faults are due to design errors, but the standard does not offer a way to identify design errors that can cause hazard.
- Good systems engineering process and software architecture design are necessary but not sufficient to ensure system safety.

Summary

- Automotive systems have changed—more complex, software intensive, more automation.
- Reductionist approach is no longer adequate.
- ISO 26262 is our latest effort to address our new challenges. It can be improved by incorporating STPA.

Proposal: Research Consortium on Automotive Functional Safety

- Industry – Government – Academia Collaboration
- Funded research projects
  - Develop a scientific framework for automotive electronics safety engineering
  - Develop a non-proprietary test bed that reflect the real world challenges
  - Educate future engineers
- Shared learning among members to
  - Improve design for safety
  - Improve industry standards
  - Support safety regulation

Thank you!

Questions?