“Commercial vehicles – Functional safety implementation process and challenges”

Dr Chitra Thyagarajan
Safety and Reliability Consultant
Mahindra Satyam
Agenda …

- Functional safety
- Importance of safety in commercial vehicles
- Need for safety compliance
- Standards related to functional safety across industries
- Process flow of ISO 26262
- Example – identifying possible hazards
- Functional safety for commercial vehicles
- Mahindra Satyam integrated engineering services overview
Functional safety

“Textbook” definition: The part of the overall safety of a system that depends on it operating correctly in response to its inputs.

Functional safety, defined as the absence of unacceptable risks due to hazards caused by the malfunction behavior of electric or electronic systems.

Functional Safety is becoming a key factor in the development of modern vehicles where the majority functions being realized with the help of sensor inputs/electrical signals and software.

Thus functional safety is specifically concerned with hazards that may result from the malfunction of one or more E/E/PE systems.

Functional Safety being a paramount design concern requires standards to be published to enable the designers for guidance and proof for compliance and Certification.
Importance of safety in commercial vehicles

- Commercial vehicles are key contributors to economic growth of a country, enabling commerce and social life to flourish.

- An accident can cause significant loss, so road safety and driver safety needs to be taken care of.

- Several active & passive safety features are developed for commercial vehicles. These functions designed using electronics and software have a critical role to play:
  - Provide assistance when required, &
  - Do not provide assistance unintentionally.

- Designing systems with adequate safety to support safe driving and avoid accidents is absolutely critical.
Need for safety compliance

✔ Changing Customer Demands:
In past customers used to ask the question - *Is the product going to work?* - *Every time? All the time?*

However, the current trend is – *Is the product Reliable and safe in all states of its functionality throughout its life cycle* (starting from concept phase up to decommissioning)?

✔ Market potential and Competition:
A Product, compliant to relevant safety standards has an edge over the non-compliant products

✔ Cost savings:
Vehicle call backs, insurance claims, product returns before the warranty
Functional safety standards across industries

- IEC 61508 - General Functional Safety
- ISO 26262 – Automotive Functional Safety
- IEC 62061, ISO 13849, ISO 15998 (earth Movers), ISO 25119 (Agriculture Vehicles) - Machinery Safety
- EN 50126/8/9 - Railway
- DO-254, DO-178C, ARP 4754, ARP 4761 – Aerospace

**Note:**
There is no specific Functional Safety standard for commercial vehicles (trucks, Buses, Trailers …). However, there are demands from commercial vehicle sector for extending the ISO 26262 for commercial vehicles and Motor cycles.
Process flow – ISO 26262

Detailed Project Plan
  ----------------------------
| Safety Plan (Confirmation Plan, Safety Case, Safety Review and Audit) |
| Item Definition |
| Impact Analysis ¹ |
| Hazard Analysis & Risk Assessment and Safety Goals |
| FSR - Functional Safety Requirement (DRAFT) |
| TSR - Technical Safety Requirement (DRAFT) ASIL Decomposition |

B

Design / System Architecture (HW/SW)
  -------------------------------------
| System FTA & System FMEA |
| FSR - Functional Safety Requirement (Review/Update) |
| Technical Safety Requirement (Review/Update) |
| Hardware & Software Safety Requirement (Detailed Design) |

C

Design Phase
  -----------------
| Hardware Safety Analysis - * |
| Hardware Testing against TSR |
| Software Testing against TSR |
| Software Safety Analysis - ** |

Review against TSR pass?
  ³
  ³

Yes

HW and SW Integration Testing
  ----------------------------------
| Functional Safety Assessment Safety case Report release |

No

* HW Safety Analysis: FMEA, FTA, SPFM&LPFM and Evaluation of Random HW Failure

** Software Safety Analysis: FMEA, FTA, ETA, Freedom from Interference

¹ Impact Analysis is required for the product which is under modification

© Mahindra Satyam 2013
Example: Hydraulic Hybrid Drive System on a refuse Truck

Designed for Fuel Saving, it Consists of

✓ 2 High pressure hydraulic Pump motors
✓ Accumulators, Oil cooler, ECU (Electronic Control Unit, Power drive unit

- At low speed vehicle uses hydraulic power. This system powers the truck from stop to stop depressurizing the hydraulic fluid every time the vehicle brakes
- At high speed say > 30mph it shifts to Internal combustion engine and ECU - controls all power drive unit functions

Possible Hazards

- Rear end Collision due to Sudden Deceleration
- Collision due to vehicle not moving with desired speed – due to vehicle not switching between hybrid system and internal combustion engine
- Fire due to temperature rise, fluid leak in accumulator

© Mahindra Satyam 2013
Functional Safety and Commercial Vehicle Safety

- One can follow ISO 26262 for the subsystems (Brakes, Steering, Engine, Chassis,…) of commercial vehicles since it is a well structured process.

- The major challenge is to assess the risk (such as Safety Integrity Levels) at vehicle level which has to be formulated with respect to the vehicle / road conditions.

- ISO 26262 – risk levels (Automotive Safety Integrity Level – ASILs) are based on the passenger cars driving conditions and controllability.

- CVSE – Commercial Vehicle Safety enforcement and several other directives exist however, they are for the vehicle safety with respect to road conditions and vehicle loads and other laws with respect to driving license, daily inspections, permissible loads etc.,

- The major challenge would be to come out with the worst case scenarios to assess a unique risk level considering the usage in different cities and countries.
Finally – A word of Caution!

We can design and build the systems with functional safety standards. prove compliance and get certified. However one should adhere to the rules and laws for safe drive with respect to vehicle limitations to avoid accidents!
Mahindra Satyam - Integrated Engineering Solutions

• 16+ years of practice maturity in ESO
• 6400+ engineers* spread across globe
• Over 20+ large dedicated engineering centers for global partners
• Delivery centers in India, China, France, Germany and USA
• Robust design methodologies: Design for safety, value engineering, reliability and six-sigma

Product Engineering Group

- 10+ years of experience working with Auto Tier-1’s and OEM’s
- Safety & reliability consulting - experts with 20+ years of experience
- Focused investments on industry experts and solutions: Steering, Braking, Occupant Safety & Driver Assist Systems
- Standards / memberships: ISO 26262 | MISRA | AUTOSAR | autospice® level 5 | GENIVI
- Active Participation in International Conference like SAE & CTI

* Engineering strength across Mahindra Satyam, Tech Mahindra and subsidiaries
Thank you.

www.mahindrasatyam.com

Safe Harbor
This document contains forward-looking statements within the meaning of section 27A of Securities Act of 1933, as amended, and section 21E of the Securities Exchange Act of 1934, as amended. The forward-looking statements contained herein are subject to certain risks and uncertainties that could cause actual results to differ materially from those reflected in the forward-looking statements. Satyam undertakes no duty to update any forward-looking statements. For a discussion of the risks associated with our business, please see the discussions under the heading “Risk Factors” in our report on Form 6-K concerning the quarter ended September 30, 2008, furnished to the Securities and Exchange Commission on 07 November, 2008, and the other reports filed with the Securities and Exchange Commission from time to time. These filings are available at http://www.sec.gov