SPECTRUM

Technology-Highlights and R&D Activities at FEV

Issue 46, March 2011

Functional Safety

Summary

In the automotive industry, electrical and electronic components are proving to be a key to the balancing act created between, on one hand, cost, emissions and fuel consumption reduction and, on the other hand, an improvement of driving pleasure, performance and safety. The vast majority of modern innovation is related to vehicle electronics and the number and complexity of distributed functions over many control units continues to increase.

Functional safety, defined as the absence of unacceptable risks due to hazards caused by the malfunction behavior of electric or electronic systems, is quickly becoming a key factor in the development of modern vehicles. It is important to notice that functional safety is a vehicle property, rather than an application domain. Functional safety is applicable to every function implemented via any electric or electronic component, independent from

Preface

Dear Readers,

as the worldwide economy continues to improve, engine and vehicle manufacturers are challenged with continuing the advancement of conventional powertrains, while investing in new technologies, especially hybrid and battery electric vehicles. In response to customer requests, FEV is likewise investing in advanced electric propulsion technology, while remembering that there is still quite some potential to improve today's powertrains.

On April 12-14, the 2011 SAE World Congress will take place in Detroit, where engine and vehicle manufacturers, suppliers, engineering development companies and academic researchers offer many glimpses of new technology. FEV is proud to be a major sponsor of the event with significant participation in the presentation of technical papers, moderating technical sessions and sponsoring the FEV Powertrain Innovation Forum.

We will also introduce several new technologies in the FEV Exhibition Booth including: an extremely downsized, parallel hybrid electric powertrain featuring a newly-developed planetary gear-set automatic transmission; FEV's Advanced Turbulence-Assisted Combustion (ATAC) CNG light-duty engine with diesel-like efficiency; and FEV's High Efficiency Combustion System (HECS) light-duty diesel engine which demonstrates extremely low CO_2 emissions and achieve 200 bar peak pressure coupled with a variable lift / variable swirl valvetrain. With customer approval, we will also exhibit examples of new production engines in which FEV played a significant development role.

There is no doubt that the next decade will proceed at a historic pace in technology advancement related to engines and vehicles. We invite you to come by and visit us at the 2011 SAE World Congress to see for yourself what the future will hold in conventional powertrains and electric propulsion systems.

Sincerely,

Gary Rogers

Executive Vice President,
FEV Motorentechnik GmbH
President & CEO, FEV, Inc.

the application domain. Functional safety goes far beyond just the scope of automotive safety-related functions, such as ABS, ESP and Inflatable Restraints. It also covers functionalities such as lighting, throttle control and active damping.

ISO 26262

This important increase in functional safety-related issues has raised the need for the automotive industry to develop its own functional safety standard. This standard, which is known as ISO 26262 is based on IEC 61508. It is a stand-alone functional safety norm and the basis for many sector-specific norms. ISO 26262 addresses the specific needs of the automotive domain. Conversely, IEC 61508 originated in the process and automation industry and is not well-suited for the automotive industry. FEV has been growing its experience with ISO 26262 since early 2007, when the standard was in its working draft status, including all of its further modifications.

The following hazards caused by the malfunctioning behavior of electric or electronic systems are taken into account as a part of the functional safety checks:

- Specification
- Implementation or realization errors
- Failure during operation period
- Reasonably foreseeable operational errors
- Reasonable foreseeable misuse

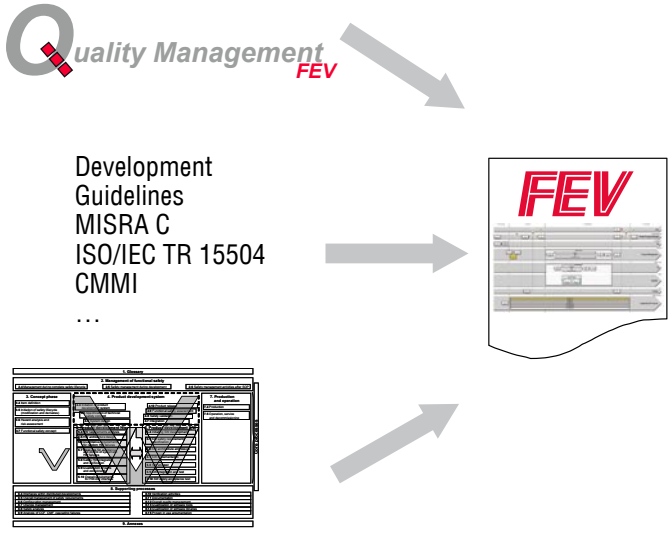

Fig. 1: FEV Safety Lifecycle

FEV has developed a safety lifecycle covering the whole project development lifecycle, supported by FEV's internal quality management rules, the CMMI development guidelines and the ISO 26262 safety lifecycle, as illustrated in Figure 1.

Risk-Based Approach
For liability reasons, the ISO 26262 followed the same risk-based approach as the IEC 61508. During the concept phase, the risk of the individual functions is assessed as a combination of the probability of occurrence and severity of risk. The risks for each hazard are assessed by determining three factors (Exposure, Controllability and Severity) and then combining them according to the table provided in Figure 2.

Source: ISO-26262

		F = Exposure x Controllability					
		1	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}
Severity	S0-No Injuries	QM	QM	QM	QM	QM	QM
	S1-Slight and Moderate Injuries	ASIL B	ASIL A	QM	QM	QM	QM
	S2-Serious, Including Lifethreatening, Injuries, Survival Probable	ASIL C	ASIL B	ASIL A	QM	QM	QM
	S3-Life-Threatening Injuries (Survival Uncertain) or Fatal Injuries	ASIL D	ASIL C	ASIL B	ASIL A	QM	QM

Fig. 2: Automotive Safety Integrity Level

This ASIL describes one of four possible classifications and specifies the quality of the necessary security requirements to fall below safety standards to an acceptable residual risk, where "D" is the highest and "A" the lowest possible classification of security-related functions. All normal sections of the ISO 26262 analysis have an ASIL dependency. The aim of implementing the ASIL is to introduce measures for sufficient avoidance of systematic failures and implement sufficient measures to mitigate risks from random hardware failures to acceptable levels.

As a subjective methodology, this risk assessment step requires some expertise so the end result is not an over-dimensioned safety specification and to keep a level of standardization in functionalities common to many different vehicles (often provided by the same supplier). FEV's experience in moderating these risk analysis sessions makes it one of the best partners for this crucial step in the development of safety related functionalities.

Supporting Processes
The introduction of measures to sufficiently avoid systematic failures raises the need to define supporting processes. The aim of these supporting processes is to avoid specification, implementation or realization errors. This is tremendously important in the automotive industry because of the complex division of work between the OEM and its suppliers.

At FEV, the necessary supporting processes, as defined by ISO 26262, are based on our experience with the CMMI development model and our CMMI Level 2 certification.

FEV's Portfolio for Functional Safety
Thanks to its early adoption of the ISO 26262 standard, FEV has developed management tools to provide the smooth implementation of the necessary safety life cycle activities in the overall project life cycle. The (safety) manager is then aware of the necessary processes required to implement in the project and the documents that are needed for each project in order to compile the necessary safety case that will show evidence that the safety of the function has been ensured.

FEV has acquired the necessary experience in assessing the risks of different safety-related functionalities. FEV has also defined safety concepts and written safety-related technical specifications for different application domains, such as gearbox automation, electric vehicle battery management systems, and hybrid electric vehicle torque management.

The FEV Quality Management business units also have experience in the development of Failure Modes and Effect Analyzes (FMEA), which are extensively used in the automotive (safety) industry both to help define technical specifications and as a design validation measures.

FEV can also act as an independent third party, conducting functional safety assessments or audits. FEV has developed a question catalogue to conduct functional safety assessments according to ISO 26262 for both the OEM and the suppliers. Both the functional safety management issues (project independent and project dependant) and the technical issues can be assessed and the results are then summarized in reports.

ogrzewalla@fev.com