A System level concepts to design ASIL C current measurement safety requirement for Battery management system using decomposition strategy.

Arpita A.Potdar.

Lear India Engineering LLP, Email ID: apotdar@lear.com

Electric vehicle (EV) has been proposed as a solution to the most daunting issue of our times, Global Warming. Yet, EV posits its own challenges like managing the high voltage Lithium Ion battery, which can cause hazards like toxic gas, fire, electric shock, thermal event in case of vehicle crash. So, an efficient, state-of-art Battery management system (BMS) design is required to prevent these hazards. Battery pack current measurement is one of the input required to calculate state-of-charge (SOC) to prevent damage or explosion of battery.

The hazard & risk analysis (HARA) for battery charge monitoring safety goal is mostly ASIL C but can change as per architecture and availability of external measures in the vehicle. The author would like to present a high-level technical safety concept (TSC) options for achieving ASIL C integrity using decomposition strategy. The decomposition strategy provides an advantage of scaling to lower ASIL level implementation in SW. e.g Microcontroller Abstraction (MCAL) and other BSW SW components can be selected of ASIL B integrity providing financial benefit. A system level decomposition also allows implementing safety mechanisms like redundancy and plausibility checks for the main safety requirement.

The FSR assumed for the high voltage current monitoring (HVCM) is “Provide correct battery pack current to master electronic control unit (ECU)”, Safe state: “No battery pack current in case of wrong current”, ASIL: C. For simplicity, the scope of HVCM is limited only to accurate battery pack current measurement with ASIL C integrity. The master ECU will be responsible to open contactors of battery pack and transition to safe state as per the output communicated from HVCM. ISO-26262- 2018 edition is used for developing the HVCM system and provide assurance that the risk of assumed safety requirement violation is “sufficiently low”.

In TSC, the main ASIL C requirement can be decomposed in ASIL B(C) + ASIL A(C) as per the rules provided in ISO-26262-9 and technical independence will be proved via analysis of failure mode in Failure mode effect analysis (FMEA), Fault tree analysis (FTA) and Dependent failure analysis (DFA).

The topologies under analysis uses a shunt and measures the current via two redundant paths with different slopes and via diverse ADC elements. Second method is the use of two hall sensors, but with different slopes in redundant path, thus establishing the technical independency. Third method considers the use of hall sensor in one path and shunt measurement in other one. The first two methods aim at proving sufficient independence using same technologies but diverse implementation. The third method uses different technologies and diverse implementations.

The approach here is for system level and it does not comment on the appropriate selection of HW component considering the battery pack max current, voltage, power dissipation and. A high-level system architecture will be presented with the above-mentioned design and its safety analysis with technical independency. As the presentation focuses on the current measurement on system level with ASIL C integrity, this approach can be used for system other than BMS also.