36th International Electric Vehicle Symposium and Exhibition (EVS36)
Sacramento, California, USA, June 11-14, 2023

Development of Electric Commercial Vehicle Torque Monitoring System for Functional Safety

Jinho Jang, Hyundoo Hwang, Haeyoun Kim

Hyundai-KEFICO, 102 Gosan-ro, Gunpo-si, Gyeonggi-do, 15849, Republic of Korea

Executive Summary

Functional safety development must be considered to ensure vehicle safety; and various technical safety concepts have been suggested for safety strategies. In this paper, as a functional safety mechanism for electric commercial vehicle, torque monitoring system and its design process are addressed on practical developer's perspective. Fulfilling technical safety requirements, we developed torque monitoring system architecture through analysis and feedback update method. Differentiated redundant torque generation process with intended functionality and fault propagation prevention logic were designed on simplified redundant architecture. On torque monitoring points, diagnostic modules were arranged for torque fault check. Proposed safety mechanism was verified by model-in-the-loop simulation back-to-back test and validated by combined architecture fault injection test.

Keywords: control system, diagnosis, electric vehicle (EV), safety, torque

1 Introduction

The acceleration of automotive electrical/electronic system complexity, for many vehicle control functions, can increase the probability of systematic errors or unintended vehicle behaviors which cause safety problems. So as to prevent such issues and assure automotive quality, safety related development and standard have been demanded by global automakers and suppliers. Safety was mainly considered as reliability of mechanical and electrical parts in the past; however, the importance of safety concept, these days, has been changed as including software logic design, not just limited in hardware.

As the most recent introduced standard, ISO-26262 is regarded as the representative and necessary development process for automotive functional safety [1]. This standard covers a whole process of automotive development: management, concept, product development, production, and analyses. So far, different types of vehicle systems and components were studied on the basis of concept level functional safety development [2-5]. In addition, several researches discussed specific and technical safety mechanisms for relevant components [6-8]. Even if many papers proposed safety concepts and their safety mechanism, practical methodology and specific concerns about logical/software development were not concretely addressed or limitedly explained, especially for vehicle control aspects.

Reinforcing these lack of industrial/academic design experience, we suggest 'Torque monitoring system' as a practical example of safety mechanism for vehicle control unit software logic. In this paper, software level product development was largely focused out of whole functional safety design process. Also, design

considerations and our development experiences are discussed on practical developer's perspective. The rest of this paper is organized as follows: brief architecture design process, practical safety mechanism logic development methodology, verification & validation, and conclusion.

2 Functional Safety based Architecture Design

In order to guarantee the functional safety of vehicle control software logic, we followed ISO-26262 development process and designed torque monitoring system. Suggested torque monitoring system was based on pre-developed control software logic; therefore, thorough analysis for existing system was carried out along with few functional safety activities: Item definition, Hazard Analysis & Risk Assessment workshop, and ASIL allocation. According to these activities, technical safety concept was introduced to achieve functional safety requirements. We considered 3-Level monitoring system, referenced by E-Gas monitoring concept [9], for technical safety concept. In this paper, only Level 2 (L2) monitoring system development was discussed as the scope of torque monitoring system. L2 monitoring architecture and safety mechanism were designed by repeated feedback updates and safety analyses: Failure Mode and Effects Analysis (FMEA) and Dependent Failure Analysis (DFA). Whole architecture design process is illustrated in Fig. 1.

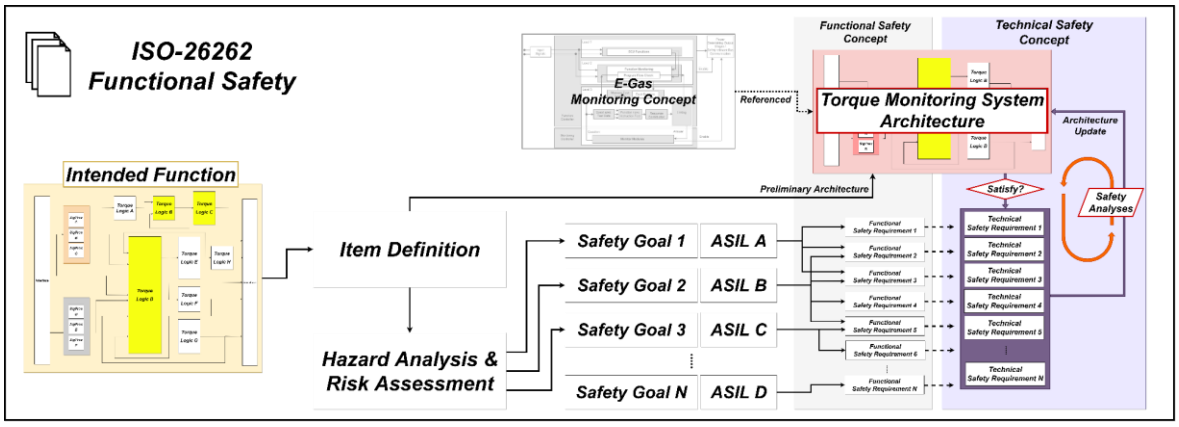


Figure1: Functional Safety based Torque Monitoring System Architecture Design Process

3 Torque Monitoring Logic Development

Proposed torque monitoring system (L2 logic) calculates differentiated redundant torques (L2 torque, T_{L2}) and these L2 torques generate tolerant torque bounds for intended function's torque (L1 torque, T_{L1}) fault diagnosis. Determined fault flags are delivered to intended function's reaction modules and let vehicle enter degradation mode or safe state. For this safety mechanism, practical L2 logic development process and methods are discussed. Overall torque monitoring system architecture is visualized as Fig. 2.

3.1 Redundancy and Simplification

Resulting from FMEA and DFA, redundant diverse software implementation needs to be developed. Since we consider torque generation process as safety related logic, torque monitoring system acts as level 2 monitoring logic to fulfill the safety requirements.

To comply with the safety requirement: Avoid identical redundant software code, draft redundant torque monitoring architecture had to be modified properly. First, we discerned redundant L2 torque generation process that imitate intended function's L1 torque generation process. Those distinguished unnecessary logics were removed and whole L2 logic was simplified; therefore, essential L2 logic was obtained avoiding exactly same redundant software from intended function (L1 logic). Simultaneously, L1 and L2 logics are not allowed to use same input data/signal, so each logic needed to be equipped with redundant interface logics. At last, L2 logic concerning data files were created and parameterized with different naming so they can be managed separately.

3.2 Torque Monitoring Points Selection and Logic Separation

Logically, vehicle safety can be achieved by fulfilling specific safety goals and their requirements. Through previous functional safety activities, we were able to select few torque monitoring points where L1 torques are compared by L2 torque bounds and L1 torques' faults are diagnosed. As a result, representative and meaningful torque points were selected in total torque generation process.

Meanwhile, we had to design separate L2 logic for preventing dependent failure effect or fault propagation. For such logic separation, selected torque monitoring points were used, like separate L2 logic's boundary points. Compared to intended function that has continuous L1 torque generation path, L2 logic torques have to be discrete and logically independent. Hence, separate L2 logic calculation process is not allowed to deliver any signal/data across the next L2 torque calculation process, which might cause cascading failures. Complementing this separate L2 logic concept, L1 torques or signals are properly delivered after data corruption check.

3.3 Differentiated Torque Generation Process

L2 torques play an important role in tolerant torque bounds generation. Depending on the similarity with L1 torques, optimality and robustness changed. Understanding the characteristics of commercial vehicles, we developed less sensitive L2 torque generation process.

For more robust torque flow generation, sampling time variation was took into consideration. We set L2 logic's sampling time longer than L1 logic's sampling time, allowing L2 torque's interpolation. Along with sampling time adjustment, time dependent operations (e.g. Differentiator, Integrator, Filter, Estimator, and Observer) and counter-related logics (e.g. Flag on/off, Stateflow mode transition) have to be modified reasonably. Affected by sampling time changes, signal processing logic's gain parameters were also needed to be tuned: Low-pass-filters and Rate limiters. Lastly, additional logic modification and value calibration were conducted for detail L2 torque shaping.

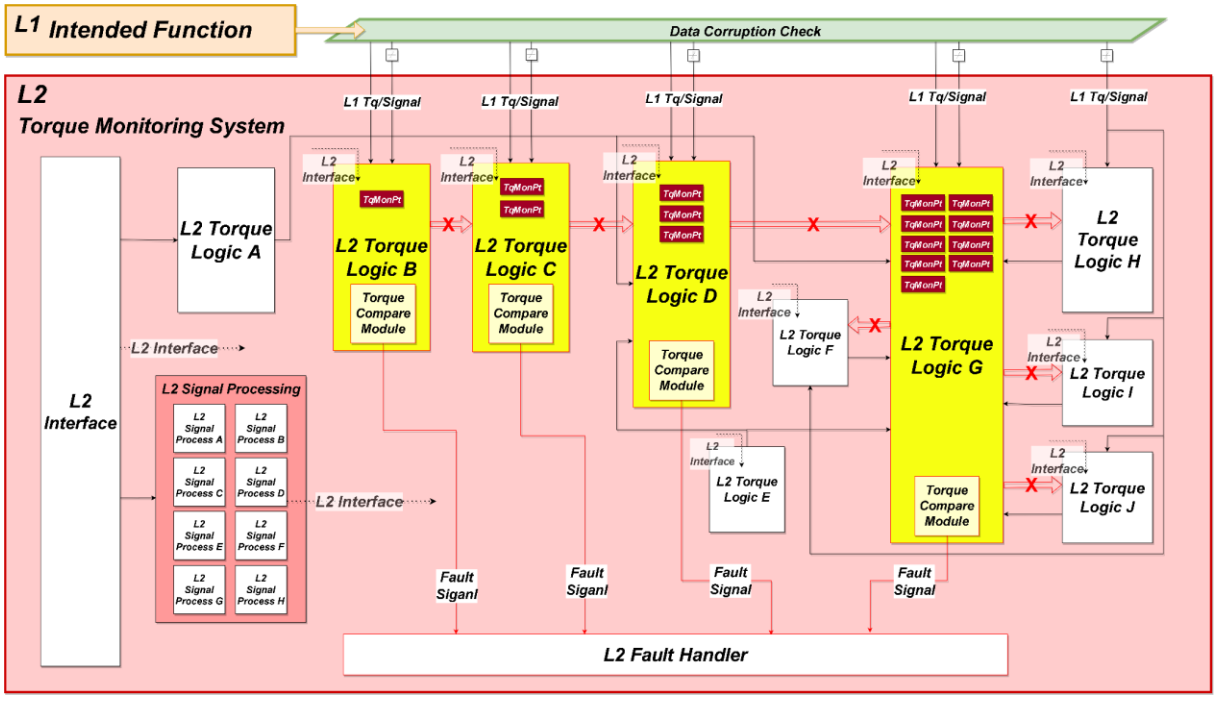


Figure2: Torque Monitoring System Architecture

3.4 Diagnostic Logic

As a final diagnostic logic of safety mechanism, L1 logic's fault is diagnosed on 'Torque compare module' at each torque monitoring point. Fault flag was designed to be activated when L1 torque exceeds L2 torque bounds and two-step offset method was proposed by our team: magnitude offset and time allowable offset.

For magnitude offset, absolute values and relative percentage margin torques were calculated on L2 torques, which generate upper and lower L2 torque bounds. As the L2 logic's sampling time was adjusted, timing errors can cause incorrect diagnosis by flag delays or one sample time difference error. In order to prevent these issues, time allowable offset was introduced. Utilizing system buffers and related logics, Torque compare modules are able to save adjacent sample times' L2 torque bounds. As a results, final L2 torque bounds are calculated by magnitude offset and time allowable offset. However, instead of securing such robustness, modules have to sacrifice the real-time. In accordance with this limitation, time-delayed L1 torques are diagnosed and proper buffer logics are designed. This limited diagnosis timing issue should be controlled within the fault tolerance time interval requirements. L2 torque bounds and diagnosis are exemplified in Fig. 3

3.5 Memory Saving Strategy

For additional design consideration, lack of memory should be concerned. In many cases, embedded system software was fully optimized to meet real-time requirements in limited hardware resource for electronic controller unit costs. Unless safety mechanism was planned in advance, enough memory allocation is hard to imagine. Especially, the exact same L2 torque calculation process with L1 occupy large amount of memory. To tackle this issue, we downsized the data type resolution of L2 logic and simplified map data. Since those method can affect the torque accuracy, fine tuning have to be followed. Otherwise, for fundamental solution, basic software level re-architecturing can be effective alternatives such as L1/L2 logic core separation and software component level optimization with minimizing inter-runnable variables.

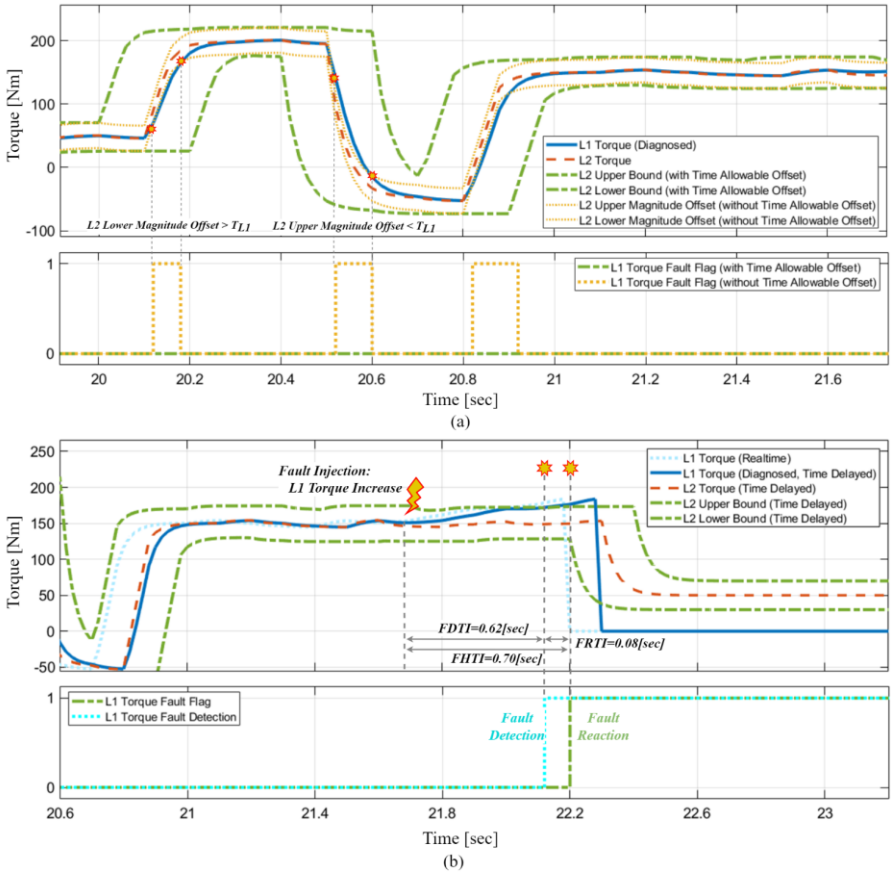


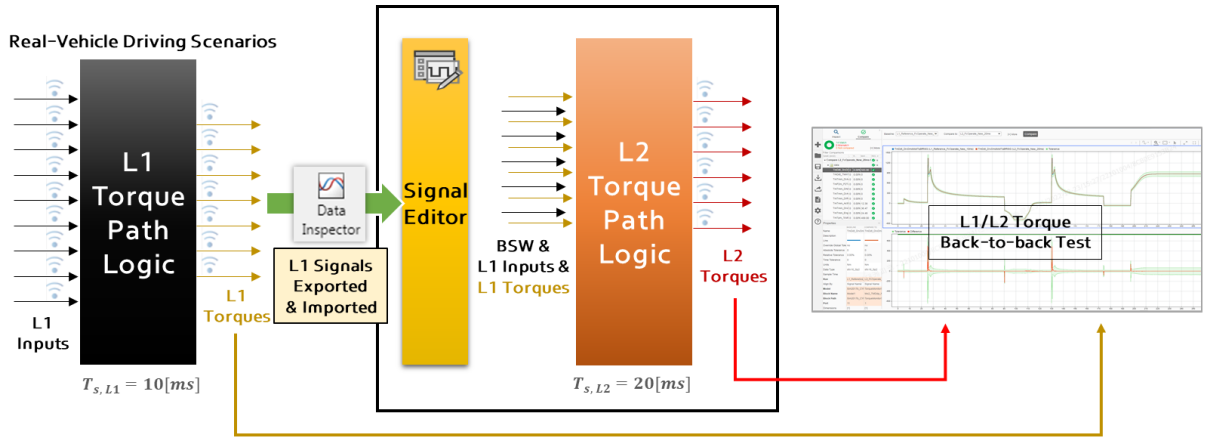
Figure3: Diagnostic Logic; (a) L2 Torque Bounds Characteristics (b) Fault Diagnosis and Real-time Torque Reaction

4 Verification and Validation

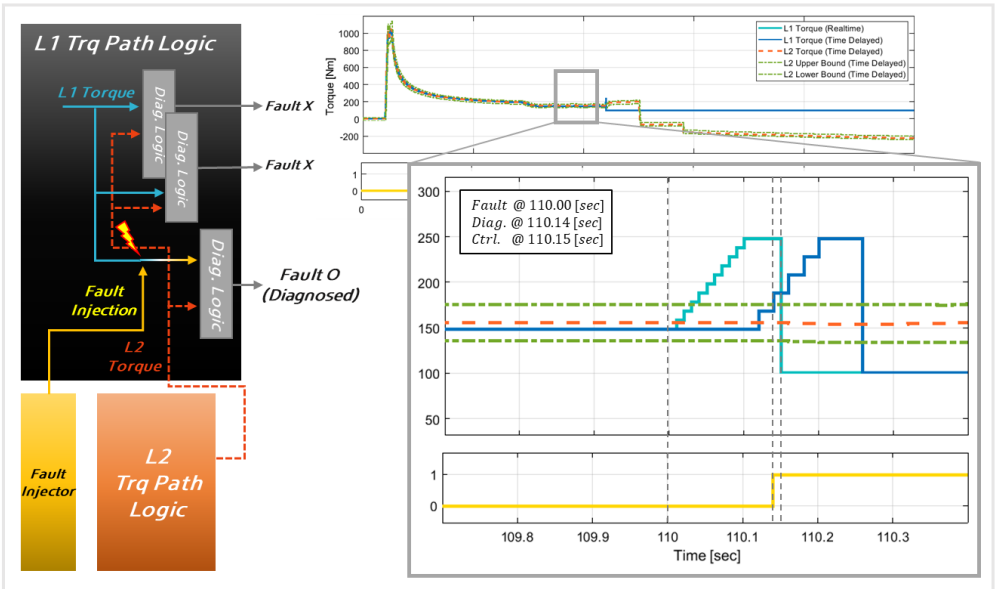
To test the developed safety mechanism, verification and validation were carried out as shown in Fig. 4

Torque monitoring system architecture and L2 logic were verified by model-in-the-loop simulation back-to-back test. Simulating real-vehicle driving scenarios' data on L1 logic, we were able to record driver's inputs and L1 input & output signals by data inspector. Next, recorded L1 signals were applied on L2 logic as same signal inputs. L2 logic outputs (torques) were compared to L1 outputs (torques) with relative tolerance and absolute offsets. Consequently, logical compatibility about torque generation process was verified on selected torque monitoring points and different driving scenarios.

For the validation of functional effectiveness, fault injection test (model-in-the-loop simulation based) was conducted on L1/L2 logics combined architecture. We injected motor torque ramp input at set time and checked how safety mechanism work. Proposed torque monitoring system detected and reacted to the fault properly, satisfying functional safety requirements (time constraints) qualitatively.



(a)



(b)

Figure4: Verification and Validation; (a) Back-to-back Test (b) Fault Injection Test

5 Conclusion

In this paper, torque monitoring system was developed as safety mechanism of functional safety ISO-26262. According to the standard and functional safety activities, functional safety concept and software architecture were designed. Detail torque monitoring system logic development process and software methodology were discussed with relevant design considerations. Lastly, torque monitoring system's modelling compatibility was verified and the safety mechanism's effectiveness was validated. As the next development process, integration test (Embedded system level) and acceptance test (Vehicle level) should be followed.

References

[1] *ISO 26262: 2018, Road vehicles—Functional safety—Part 1-12,* International Organization for Standardization (ISO), 2018-12

[2] Christiaens, S., Ogrzewalla, J., and Pischinger, S., *Functional Safety for Hybrid and Electric Vehicles*, SAE Technical Paper 2012-01-0032, 2012

[3] Li, S., Chang, C., and Zhao, H., *Functional Safety Development of E-motor Drive System for PHEV*, SAE Technical Paper 2015-01-0261, 2015

[4] Yongqiang, Zhao, Li Chang, and Li Xiang. *Development of the safety diagnosis system for VCU of pure electric vehicle*, Journal of Physics: Conference Series. Vol. 1605. No. 1. IOP Publishing, 2020.

[5] Y. Dajsuren and G. Loupias, Safety Analysis Method for Cooperative Driving Systems, 2019 IEEE International Conference on Software Architecture (ICSA), Hamburg, Germany, 2019, pp. 181-190, doi: 10.1109/ICSA.2019.00027.

[6] A. Köhler and B. Bertsche, *Evidence of the Effectiveness of Cyclic Technical Safety Mechanisms*, in IEEE Access, vol. 9, pp. 82188-82198, 2021, doi: 10.1109/ACCESS.2021.3085662.

[7] T. Bijlsma et al., *A Distributed Safety Mechanism using Middleware and Hypervisors for Autonomous Vehicles*, 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 2020, pp. 1175-1180, doi: 10.23919/DATE48585.2020.9116268.

[8] T. Schmid, S. Schraufstetter, S. Wagner and D. Hellhake, *A Safety Argumentation for Fail-Operational Automotive Systems in Compliance with ISO 26262*, 2019 4th International Conference on System Reliability and Safety (ICSRS), Rome, Italy, 2019, pp. 484-493, doi: 10.1109/ICSRS48664.2019.8987656.

[9] *Standardized E-GAS Monitoring Concept for Gasoline and Diesel Engine Control Units,* EGAS Workgroup, version 6.0, 2015-07-13

Presenter Biography

Jinho Jang is a research engineer at Hyundai KEFICO. He holds a M.Sc. degree in Automotive Electronic Control Engineering, obtained at Hanyang University, Seoul, Korea. His research topics include control engineering and application/basic software development for electrified vehicle control. Currently, he is involved in a functional safety development project for electric commercial vehicles.