Poster: Network-Centric Approach Using Task Migration for Drive-by-Wire Vehicle Resilience

Jeanseong Baik, Haegeon Jeong, and Kyungtae Kang
Dept. of Computer Science and Engineering, Hanyang University, Republic of Korea
{jsbaik, haegeonj, ktkang}@hanyang.ac.kr

***Abstract*—The electronic control unit (ECU), considered the brain of a vehicle, suffers from a design problem called single point of failure (SPOF), which can induce system malfunctions. This problem can be addressed via redundancy, which increases the reliability of a mission-critical system by allowing multiple ECUs to perform a single function. However, this solution requires additional ECU and maintenance costs incurred by the redundant ECUs. A cost-effective approach for improving safety is to utilize the network connectivity between existing ECUs. In this paper, we propose a method that migrates critical tasks residing in an infeasible ECU to a replaceable ECU by using the network connection between them. Furthermore, to demonstrate the feasibility of the method, we implemented a task migration method on a Lego vehicle composed of three ECUs to prevent sudden unintended acceleration accidents caused by faults in an ECU managing the acceleration task.**

***Index Terms*—Task migration, Redundancy, Resilience, High reliability**

I. Introduction

The electronic control unit (ECU), the brain of the vehicle, suffers from a design problem called single point of failure (SPOF), which can induce system malfunctions. This problem is addressed via redundancy, which increases the reliability of a system via primary-backup replication at the expense of increased costs incurred due to extra ECUs. Because these costs are passed on to customers, vendors avoid using redundancy. By saving on costs, current vehicle systems are not actively handling the safety accidents. One common accident is ECU failure, where moisture infiltrates inside the unit and eventually produces unexpected acceleration. This ECU failure can cause collisions with obstacles and life-threatening accidents.

Accordingly, a cost-effective approach for improving safety is to utilize the network connectivity between existing ECUs without the need for additional ECUs. Vehicles already have up to 80 mutually connected ECUs, which can interactively control and monitor others to extend the troubleshooting scope for the failure. This network connectivity provides a safe environment for vehicle systems to overcome potential accidents caused by SPOF.

This work was supported in part by the Institute of Information & Communications Technology Planning & Evaluation (IITP) Grant funded by the Korean Government (MSIT - Ministry of Science and ICT, No.2014-3-00065, Resilient Cyber-Physical Systems). This Research was also supported in part by the Next-Generation Information Computing Development Program through the National Research Foundation of Korea funded by the MSIT under Grant 2017M3C4A7083676.)

978-1-7281-6992-7/20/$31.00 ©2020 IEEE

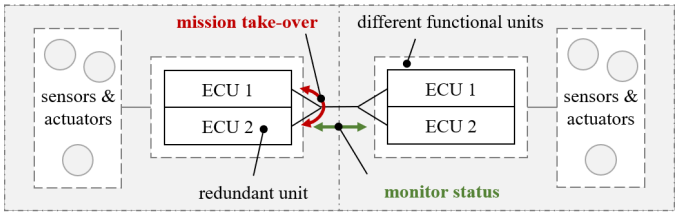

Fig. 1. Structure of a generic by-wire system; ECU: Electronic Control Unit

In this paper, we propose a method that migrates critical tasks residing in an infeasible ECU to a replaceable ECU using their network connectivity, which provides seamless services in the presence of ECU errors. Moreover, to demonstrate the feasibility of the method, we implemented a task migration method on a Lego vehicle composed of three ECUs to prevent sudden unintended acceleration (SUA) accidents caused by the fault of an ECU managing the acceleration task.

II. Conventional Redundancy Methods

Figure 1 provides a general view of drive-by-wire systems [1], which employ a conventional primary-backup approach to address the SPOF, by introducing replications for each primary ECU. When all redundant ECUs are turned on, the system operates in a hot standby mode, reducing the need to boot or initialize redundant devices, thereby decreasing the take-over time at the expense of maintenance cost. Another method of addressing SPOF is a network-centric approach [2], which eliminates hardware duplication; if a particular ECU fails, then the other ECUs detect the failure and continue the adjustment operation accordingly as a fail-safe. Although this method can reduce the number of ECUs required, its goal was limited to fault detection, and providing error resilience, by means of mission taking over, was not a primary concern. Finding an ultimate solution and designing a vehicle safety system that simultaneously satisfies both goals of reducing cost and assuring safety with no service interruption remain challenging. In a study combining the two methods mentioned above, a MOBILE [1] vehicle project has made significant progress in providing an approach that meets both cost and safety requirements but has not progressed to specific methodologies or implementations.

III. Our Approach

The proposed method based on task migration across ECUs is shown in Figure 2. It is used when ECUs with distinct