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.

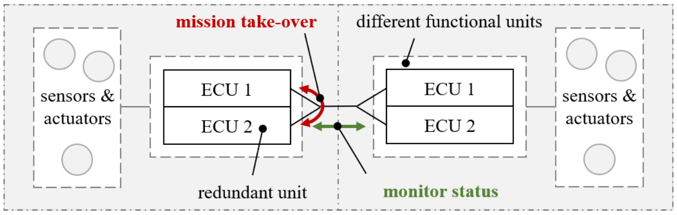

Fig. 1. Structure of a generic by-wire system; ECU: Electronic Control Unit

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

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

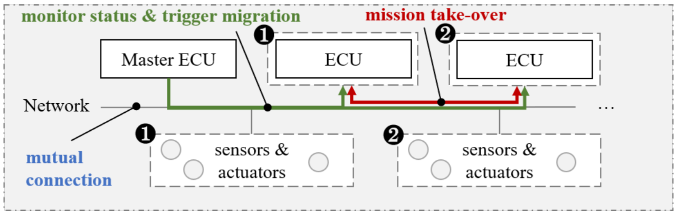

Fig. 2. Structure of a mutually connected system using migration method

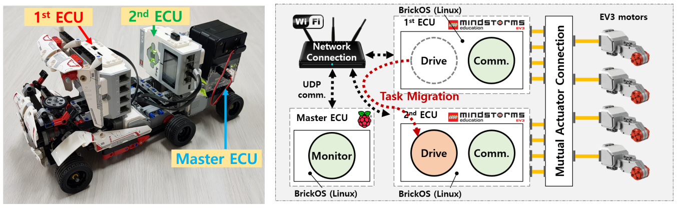

Fig. 3. Implementation and structure of EV3 multi-node vehicle

functions are mutually connected in a single system where the mission can be resumed by another ECU due to an ECU failure. It uses a migration table stored in the master ECU, which a key data structure to map the task migration to a replaceable ECU. Our method can be used on multi-ECU systems in which ECUs with distinct actuators are mutually connected. Updating the migration table dynamically allows the tracking of the ECUs on which the migrated task runs when those ECU are consecutively disrupted. Additionally, our live-migration method has benefits in terms of both cost and safety assurance, by maintaining the important context of running tasks for uninterrupted services.

Another feature of the proposed method is that it considers multi-factors, such as criticality of the task and capacity of the ECU, implemented with a *linked list* data structure. All the tasks are classified according to their criticality, and migrating the task from an erroneous ECU is permitted when the task has higher criticality than those running on a replaceable ECU to maintain the high reliability of the overall system, unless the replaceable ECU has sufficient capacity to accommodate migrated tasks without interrupting existing running tasks. For this purpose, the migration table inside the master ECU maintains information about all the tasks and their criticality on each ECU, adjacency of all the ECUs, and their capacities.

IV. Evaluation

We implemented the basic structure of the proposed method in an EV3 Lego vehicle, as shown in Figure 3. The Raspberry Pi 3 associated with the EV3 module is the master ECU; it monitors the failures of other slave ECUs and maintains critical tasks by selecting alternative ECUs in the task migration table that holds the entire ECU information. The vehicle's task migration technique reads the information about the task and uses a Linux tool called *ptrace* [3] to maintain the transfer speed of the car. The task migration algorithm was implemented to recover from SUA. There are two main contributions to this method.

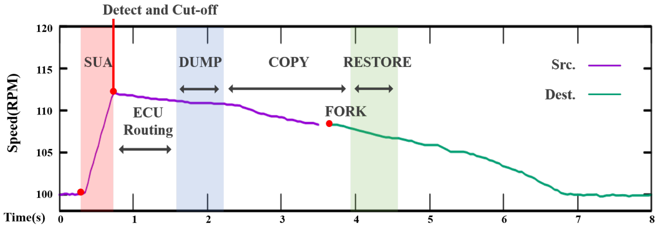

Fig. 4. Sample application of avoiding SUA using migration method

First, our approach is cost-effective because it minimizes the number of ECUs used while achieving the same safety performance as the traditional redundancy technique. Suppose that a redundancy technique is applied to construct a 100% safe system using two ECUs per task. However, if the tasks of each ECU can replace each other, then the number of ECUs is reduced because the units are redundant. The total number of ECUs is given as $2N - \sum_{\tau=1}^{N} \texttt{Replace}(\tau) * \texttt{Capacity}(W_\tau)$. This minimizes the cost of redundancy $2N$, where N is the number of tasks, and the function $\texttt{Replace}$ is the existence of the replaceable ECU for a given task τ. Furthermore, the resource capacity is an essential function because the replaceable ECU should accommodate the workload of the migrated task W_τ, including the existing running task.

Second, our approach provides non-disruptive service to ensure safety because it maintains the main state of the previous task. As shown in Figure 4, the destination ECU takes over the driving mission during SUA caused by a fault in the source ECU and stabilizes the speed in 6 seconds. This uninterrupted take-over is comparable with the existing restart-based redundancy method.

V. Conclusion

In this study, we implemented a task migration method on a single Lego vehicle with three EV3 controllers to utilize a resilient system that recovers dead-end functions to avoid collisions. To overcome the limitations of the SPOF, we utilized the network connectivity of ECUs and used task migration techniques between ECUs to sustain the critical functions. The method has three main advantages. First, it maintains the main state of the previous task. Second, whenever a master ECU detects a fault with an observed ECU, it will identify a replaceable ECU dynamically. Finally, unlike redundant systems, it is cost-effective because this method guarantees safety using existing mutually connected ECUs without redundant ECUs.

References

[1] P. Bergmiller, "Design and Safety Analysis of a Drive-by-Wire Vehicle," in *Automotive Systems Engineering*, Berlin, DE: Springer, 2013, pp. 147–202.

[2] A. Gujarati, M. Appel, and B. B. Brandenburg, "Achal: Building highly reliable networked control systems," in *Proceedings of the International Conference on Embedded Software*, New York, US, Oct. 2019.

[3] S. Kashyap, C. Min, B. Lee, T. Kim, and P. Emelyanov, "Instant OS Updates via Userspace Checkpoint-and-Restart," in *USENIX Annual Technical Conference*, Denver, CO, June 2016.