Transactions of KSAE, Vol. 31, No. 2, pp.143-151 (February, 2023)

pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2023.31.2.143

리던던시 환경에서 Steer-by-Wire 시스템의 중재 제어 방법에 관한 연구

김 대 성* · 이 진 환

HL 만도 SW캠퍼스 SW 1랩

A Study on Arbitration Control Method of Steer-by-Wire System in Dual Redundancy Environments

Daesung Kim* · Jinhwan Lee

SW 1 Lab, SW Campus, HL Mando Corporation, 21 Pangyo-ro 255beon-gil, Bundang-gu, Seongnam-si, Gyeonggi 13486, Korea
(Received 5 April 2022 / Revised 5 July 2022 / Accepted 25 October 2022)

Abstract：Reliability is described as a probability that a system will operate properly for a defined length of time without any failures, and is considered as one of the important design attributes. Safety critical devices, such as the Steer-by-Wire, should be considered as redundant E/E architectures that are configured as two identical controllers to ensure higher functionality, which is further defined as reliability that can recover from any failures. Two identically configured controllers should swap a role in the redundancy scheme within the deadline when a system detects a fault. A challenge to dynamic redundant systems is to determine a precise role in the active controller to operate a system, to detect errors in the active controller, and to take over as a backup controller in the defined time. This paper studies dynamic redundant architectures and arbitration control methods that can provide full fault-tolerance without any deviation in functionality even in the occurrence of faults.

Key words：Steer-by-wire(전기신호식 지능형 조향 시스템), Steering system(조향 시스템), Arbitration control(중재 제어), Redundant control system(이중화 제어 시스템), Fault-tolerance(결함 허용), Mutual exclusion(상호 배제), Deadlock (교착상태), Semaphore(세마포어), Binary arbiter(바이너리 중재 제어 모듈)

Subscripts

SbW	: steer-by-wire
SFA	: steering feedback actuator
RWA	: road wheel actuator
EPS	: electric power steering system
E/E	: electrical and electronics
ECU	: electric control unit
CAN	: controller area network
IMC	: inter-micro communication
ASIL	: automotive safety integrity level
SG	: safety goal
FTTI	: fault tolerant time interval
HARA	: hazard analysis and risk analysis
HMT	: hazard metric test
ME	: mutual exclusion
CCF	: common cause fault
CRC	: cyclic redundancy check
RTE	: runtime environment
PMSM	: permanent magnet synchronous motor
CCA	: circuit card assembly
MCU	: micro controller unit

1. 서 론

최근 자율주행, 차량 지능화 등 산업의 E/E 시스템 기술 발전과 함께 제동, 전동식 파워 조향 시스템과 같은 차량의 주요 안전 섀시 시스템의 치명적인 결함에 의해

*A part of this paper was presented at the KSAE 2021 Spring Conference

*Corresponding author, E-mail: daesung2.kim@hlcompany.com

운전자가 위험한 상황에 처하는 것을 방지하기 위해 2차 또는 예비 안전 메커니즘을 필요로 한다. 특히, 자율주행, 무인자동차 환경에서 요구되는 E/E 시스템의 기능성, 가용성 및 신뢰성을 향상시키기 위해 안전 메커니즘이나 이중화 아키텍처를 운용하게 된다.[1] 자동차 산업에서 대부분의 이중화 시스템 아키텍처는 기능 안전 요구사항에 따라 시스템 기능 안전 목표 수준의 전체적인 Fault-tolerance 요구를 달성할 수 있도록 설계된다. 이중화 시스템 아키텍처의 핵심기술은 중재 제어(Arbitration Control) 모듈로서 동작 성능, 시스템 운용 성능, 결함 감지 시 운용 모드 전환, 운전자의 안전 상태 유지 등 시스템 주요 기능의 신뢰성을 결정한다. 이중화 E/E 시스템의 중재 제어 전략은 이미 기계 시스템 산업, 자동차, 항공기, 항공 교통 제어, 전력 시스템 및 기타 많은 분야를 제어하는 다양한 산업에 폭넓게 활용되고 있다.[2]

현재의 기구연결식 전동 조향 시스템(EPS)은 토크 센서, 전자 제어 모듈(ECU), 영구 자석 동기 모터(PMSM), 피니언 각도 센서 및 기타 기계적 부품(예: 감속 기어, 랙, 피니언)으로 구성된다. 토크 센서 모듈은 기본적으로 조향 토크를 측정하고 ECU에서 운전자 피드백 소스의 역할을 하는 신호를 보내는 데 사용된다. ECU의 모터 제어는 조향 토크를 추정하여 제어하도록 설계 되어 있으며 모터 위치 센서는 피니언 각도 위치를 추정하는데 사용된다. 이 같이 ECU에 의해 계산된 어시스트 전류는 운전자가 의도하는 방향으로 조향 휠을 더 쉽고 편하게 움직일 수 있도록 도와준다.[3]

이러한 전기/전자적 구성 요소를 갖는 시스템에서 결함 발생은 전동식 파워 조향 시스템의 기능 또는 성능 제약으로 이어질 수 있기 때문에, 시스템의 신뢰성과 가용성은 운전자와 보행자에게 중요한 지표로서 고려되어야 한다. 현재 대부분의 조향 시스템 설계는 결함에 의한 위험을 최소화하기 위해 안전 메커니즘 및 조치에 초점을 맞추고 있다. 이러한 설계 활동은 조향 시스템이 결함에 의해 갑자기 완전히 기능이 상실되는 것을 방지하는 데 효과가 있을 수 있지만, 차량의 모든 환경과 조건에서 운전자의 안전을 담보하기에는 상당히 제한적이다. 이 한계를 극복하기 위해 시스템 동작 중 결함 발생 시에도 시스템의 어떠한 기능 저하없이 성능을 유지할 수 있는 E/E 시스템의 이중화 아키텍처는 필수이다. 특히, Fig. 1에서 보는 바와 같이 컬럼과 랙 사이에 기구적 연결이 없는 SbW 시스템에서 E/E 결함은 조향 기능 상실을 만들어 운전자에게 치명적 위험을 줄 수 있는 잠재적 위험을 가지고 있기 때문에 E/E 시스템의 이중화 아키텍처는 필수적으로 요구된다. 그렇지 않을 경우, 운전자와 보행자들은 매우 위험한 상황에 노출될 수 있다.

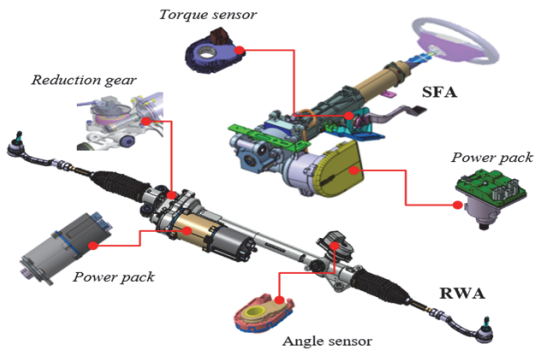


Fig. 1 System configuration of steer-by-wire

본 논문에서는 SbW 제품의 E/E 이중화 제어 시스템 아키텍처 운용 성능과 품질을 결정하는 중재 제어 방법을 제안하고 평가, 검증한다. SbW 시스템은 프리미엄 조향 성능을 제공하기 위해 가상 시스템을 기반으로 조향 성능을 빌드하는 전동식 조향 반력 장치(SFA)와 운전자의 조향 의도를 차량 바퀴에 전달하여 바퀴를 움직이는 차륜 조향 장치(RWA)로 구성된다. 본 연구의 주요 기여는 (1) SbW 제품에 적용된 E/E 이중화 제어 시스템의 아키텍처 제안과 운용 전략, (2) 리던던시 환경에서 SbW 이중화 시스템의 최적화된 중재 제어 알고리즘 설명, 평가, 검증이다. 끝으로 본 과제의 궁극적인 목적은 리던던시 환경에서 E/E 이중화 제어 시스템의 안전적인 중재 제어를 통해 SbW, EPS와 같은 주요 안전 제품의 신뢰성, 기능성, 가용성, 강건성을 향상시키기 위한 것이다.

본 논문의 구조는 다음과 같이 구성된다. 2절에서 현재의 기구연결식 전동 조향 시스템의 잠재적 위험 분석 및 안전 조치 기술에 대해 설명하고, 3절에서는 SbW 시스템 신뢰성 향상을 위한 E/E 이중화 제어 시스템 아키텍처와 중재 제어 전략에 대해 제안한다. 4절에서는 리던던시 환경에서의 E/E 이중화 제어 시스템의 결함 감지 및 조치에 대한 기능 안전 목표 및 검증 결과를 보여준다. 마지막으로 5절에서 결론을 도출한다.

2. 조향 시스템의 안전 분석과 조치 및 관련 연구

조향 시스템의 기능 안전 분석은 기본적으로 ISO 26262 절차에 따라 수행한다. 조향 시스템의 안전 목표(SG)는 HARA 분석을 기반으로 자동차 안전 무결성 수준(ASIL)을 산정하여 도출한다. 차량의 Lateral 모션과 운전자의 조향 Effort 기준에 따라 다음 주요 세 가지 항목으로 조향 시스템의 중대한 위험을 정의할 수 있다.[4]

- Unintended steering: 운전자의 의지와 관계없이 예기치 않은 조향 움직임(Reverse steering 포함)
- Locked steering: 운전자에게 과도한 Effort를 요구하거나, 완전히 잠긴 상태
- Excessive steering: 운전자가 요구한 것보다 과도한 조향 어시스트 출력

Table 1은 그 결과를 토대로 도출된 조향 시스템의 기능 안전 목표와 예비 안전 메커니즘(안전한 상태)을 보여준다. SG-5 sudden loss of assistance는 아직 중대한 위험으로 분류되지 않았으나, 여성이나 노약자 등 취약 계층들에게 위험 상황으로 노출될 수 있는 우려로 일부 자동차 제조사들은 High ASIL을 요구하고 있으며 현재의 안전 상태인 Manual steer 역시 전기적 조향 어시스트를 유지할 수 있게 하는 추세이다. Fig. 2는 어떠한 경우에도 안전 목표에 따라 운전자에게 안전한 조향 어시스트 상태를 제공할 수 있게 하는 시스템 상태 천이도를 보여준다. 안전 모드 상태에서 운전자는 시스템 성능 제한으로

Table 1 Safety goals of a conventional steering system

Id	Safety goals	ASIL	Safe state
SG-1	Unintended steering assistance shall be prevented	D	Manual steer
SG-2	Locked steering shall be prevented	D	Manual steer
SG-3	Reverse steering shall be prevented	D	Manual steer
SG-4	Excessive assistance shall be prevented	D	Manual steer
SG-5	Sudden loss of assistance shall be prevented	B	Warning indication

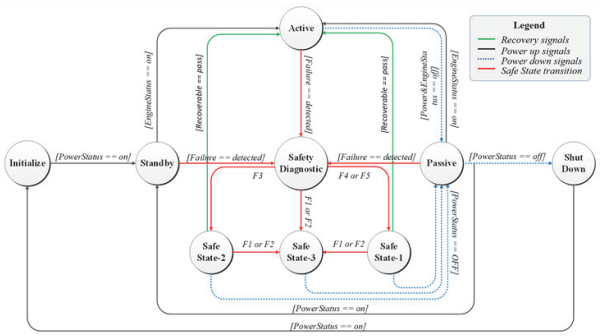


Fig. 2 System safe state transition based on failure level
(1) F1: Permanent fault types or non-recoverable faults
(2) F2: Critical severity faults
(3) F3: Limited recoverable faults
(4) F4: Recoverable faults
(5) F5: Benign faults

인해 의도하지 않은 조향 동작이나 성능을 경험하지 않도록 해야 한다.

(1) 시스템은 전원이 차단될 때까지 안전 상태-3(Safe State-3)에서 다른 작동 상태로 전환되지 않아야 한다.
- 결함1(F1)은 영구적인 결함 유형이며, 전원 주기(Off→On)가 감지되거나 에러 코드가 삭제될 때까지 안전 상태가 유지되어야 된다.
- 결함2(F2)는 잠재적으로 위험한 상태를 유발할 수 있는 중대한 결함으로 상태 변화가 없어야 한다.
- 결함3(F3), 결함4(F4), 결함5(F5)는 조향 시스템의 성능 저하를 초래할 수 있는 결함으로 회복 가능해야 한다.

(2) 안전 상태 전환 제한은 다음과 같이 정의된다.
- 시스템 결함 발견 시 안전 상태-1(Safe state-1)에서 안전 상태-2(Safe state-2)로 전환해야 한다.
- 시스템 결함 발견 시 안전 상태-1에서 안전 상태-3으로 전환해야 한다.
- 시스템은 결함이 제거될 경우 안전 상태-1 또는 안전 상태-2에서 정상 동작으로 전환되어야 한다.
- 기본적으로 시스템은 안전 상태에서 초기화 되어야 하며, 안전 상태의 모터 제어 토크는 0이다.
- 초기화 중 시스템은 대기모드 상태여야 한다.
- Power-On Reset은 시스템 상태를 초기화 상태로 전환해야 한다(정상 및 비 정상 Power-On Reset).
- 모든 제어기의 Non-Power-On Reset은 시스템 상태를 안전한 상태로 유지해야 한다(모든 예외 사항은 실행 중인 재설정을 유발할 수 있으며 제어기에 내장되어 있다).
- 시스템은 초기화 중에 F1 결함이 감지될 경우 정상 동작으로 전환되지 않도록 설계되어야 한다.

앞서 언급했듯이 Table 1에 기술된 조향 시스템의 예비 안전 메커니즘은 전기적 조향 어시스트가 없는 운전자의 핸들과 랙 사이의 기계적 연결부로 운전자에게 장시간 노출될 경우 조향 조작 부담을 증가시킬 수 있는 기능적 한계를 지니고 있다. 이로 인해 최근에는 기구적 연결에 의한 제한된 조향 조작은 위험 상황으로 인식되기 시작했다. 그리하여 결함이 있는 경우에도 제한적인 E/E 시스템 성능을 유지할 수 있게 하기 위해 추가 하드웨어 구성 전략이나 소프트웨어 알고리즘 등을 이용한 다양한 Fault-tolerance 기법이 연구되고 있다.

특히, SbW 시스템은 컬럼과 랙 사이에 기계적 연결이 없는 “By wire” 구조로서 결함 발생 시 최악의 경우 조향 기능 상실로 인해 운전자와 보행자 모두 큰 위험에 처할 수 있기 때문에 유사 시 Backup 동작의 신뢰성이 매우 중요하다. 현재 대부분 SbW 시스템의 기능 안전 및 신뢰성

에 대한 연구는 결함 발생 시 위험을 최소화하기 위해 Brake, ESC 시스템과 같은 차량 동적 모델을 이용하여 운전자의 조향 의지를 판단하는 예측 모델 기반의 제한적 Backup 동작을 구사하는 전략이다.[1] 이는 예측 제어에 의한 제한적인 조치로 일시적인 위험을 줄이는 것은 가능할 수 있으나, 기능 안전 목표에 부합한 지속적인 조향 기능 제공에 한계가 있어 2차 사고의 잠재적인 위험성을 가질 수 있다. 더욱이, 자율주행 모드에서 조향 시스템은 운전하는 동안 결함이 감지되더라도 어떠한 기능 제약 없이 운전자에게 정상적인 조향 성능을 제공해야 하는 것이 필수 요구사항으로 기계적 연결에 의존하는 LoA(Loss of Assistance) 나 예측 기반 제어 모델은 예비 안전 메커니즘으로 사용하기에 많은 제약을 가지고 있다. 이에 하드웨어 기반 E/E 제어 시스템의 이중화는 운전자를 포함한 공공의 안전을 위해 결함 발생 시에도 시스템 본래의 성능을 지속 유지할 수 있도록 필수적으로 고려되어야 한다.

3. E/E 시스템의 이중화 아키텍처와 바이너리 중재 제어

E/E 시스템의 이중화 아키텍처 모델은 이미 다양한 산업 분야에서 활용되고 있는 기술로 용도, 목적에 따라 다르게 정의될 수 있지만, 기본적으로 제어 시스템 아키텍처를 구현하기 위한 설계 철학이나 시스템 접근 방식에 의해 결정된다.[5,9] 이중화 된 E/E 시스템의 상세 설계 관점에서 중재 제어 모듈은 시스템 운용을 총괄하는 중요 모듈로서 결함 정보, 2nd ECU(Backup 제어 모듈) 상태, 자신의 상태, 동기화 등 수 많은 동적 입력 정보를 받아 시스템 동작 상태를 결정한다. 본 논문에서는 높은 신뢰성을 요구하는 복잡한 SbW 제품을 위한 E/E 이중화 제어 시스템 아키텍처와 그 환경에서 안전하게 활용 가능한 중재 제어 방법을 제안하고 평가했다.

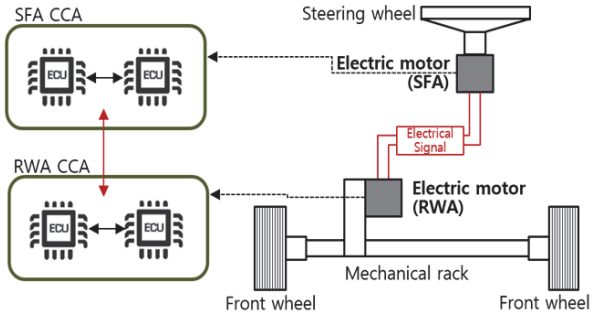


Fig. 3 Redundant system configuration with two identical controllers in steer-by-wire

3.1 SbW E/E 이중화 제어 시스템의 구성

SbW E/E 제어 시스템은 이중화 된 센서와 제어기, 이중 권선 모터로 구성된 SFA, RWA 두 개의 서브 시스템으로 구성된다. 각 서브 시스템은 두 개의 동일한 ECU와 지속적으로 통신하는 신뢰성 있는 내부 MCU 간 CAN 통신(IMC CAN)과 차량 통신을 위한 Dual Vehicle CAN(Controller Area Network) 네트워크 토폴로지로 구성된다.

Fig. 3에서 각 SFA, RWA는 동일한 두 제어기는 회로 부품 어셈블리보드(CCA) 상에 마이크로 컨트롤러 유닛(MCU) 중심으로 연결된 2개의 하드웨어 블록(ECU)으로 구별된다. 중재 제어 모듈은 동일한 두 제어기 간의 상호 배제(Mutual exclusion) 상태가 보장되는 시스템 운용을 제공한다. 시스템 동작 초기에 각 제어기의 최초 Role 결정 이후, 각 제어기의 정보는 IMC CAN 통신 기반 주기적으로 상호 정보를 공유하는 방식으로 시스템 동기화 및 Role 결정을 수행한다. 이중화 제어 시스템의 가용성을 높이기 위해 각 제어기는 외부 Vehicle CAN 네트워크를 구성하고 IMC CAN의 중요 메시지를 외부 CAN을 통해 공유한다. CAN Bus에 실리는 기능적으로 ASIL D 요구 메시지들은 CRC-16 checksum을 사용하여 메시지의 무결성을 보장한다. Fig. 4에서는 SbW 시스템에서 SFA와 RWA 간 협업 네트워크를 보여주는 것으로 중재 제어 모듈의 이중화로 서로 다른 서브 시스템 상태를 관찰함으로써 SbW 시스템의 가용성을 더욱 향상시킬 수 있다. 두 개의 제어기와 이중화 된 토크 센서가 포함된 SbW 시스템은 기능 안전 요구사항에 따라 ASIL-D 등급에 맞게 설계되어야 한다.[8,10] 또한, 동일한 두 제어기 사이의 중재 제어에 사용되는 IMC CAN 통신 버스는 공통 원인의

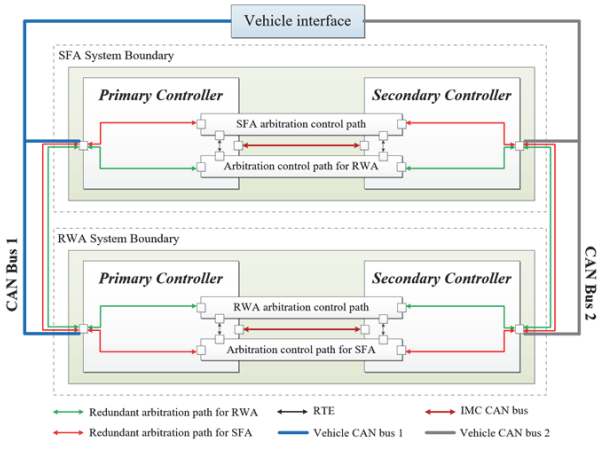


Fig. 4 Electrical redundant systems with two identical controllers in steer-by-wire

결함(CCF)을 가질 수 있어 이중화 시스템의 무결성을 달성하기 위한 통신 대안이 고려되어야 한다. 이러한 CCF 약점을 보완하고 IMC CAN 통신의 신뢰성을 높이기 위해 각 제어기에서 외부로 연결되는 Dual CAN 버스 네트워크를 구성하여 사용한다. 더불어 두 개의 동일한 제어기는 외부 게이트웨이 장치에 서로 연결된 외부 Vehicle CAN 버스를 통해 차량 정보를 이용하여 시스템의 기능성을 향상시킬 수 있다.

시스템 안전을 위한 기능 운용의 예로서 Active 상태 제어기가 심각한 시스템 결함을 감지한 경우, 요구하는 시스템 데드라인 내 Active 제어기의 Role을 Backup 제어기로 전환해야 한다. 본 연구에서 제안하는 중재 제어 모듈은 기본적으로 시스템 운용을 위한 시스템의 의도치 않은 중복 제어, 공유 리소스 동시 접근, 제어기 Role 결정, FTTI 문제를 해결하는 데 사용되는 동적 세마포어 알고리즘을 가지고 있다. 중재 제어 모듈은 다음과 같은 기능을 수행한다.[12)]

- 각 제어기의 Active, Backup 상태 유지
- 제어 모드 및 시스템 시퀀스의 동기화 관리
- 상태 정보를 수신하기 위해 각 제어기로 정기적 Heartbeat 요청 전송
- Backup 제어기 Role을 부여하여 Backup 제어기를 Active 제어기로 인계할 준비 상태
- 데드라인 및 시스템 수행 시간을 제어
- 두 개의 동일한 제어기의 ME 상태 독립성 보장
- 결함이 있을 때마다 제어기에 동작 상태 설정 지시
- 예비 전원 공급 스위치에서 정상적으로 닫힌 스위치를 구동하기 위한 공급 전압 출력을 사용하여 각 제어기의 전원 공급 제어

3.2 세마포어 이용한 중재 제어

두 개의 제어기가 존재하는 이중화 시스템에서 중요한 것은 시스템 운용을 결정하는 제어기 사이의 중재 제어이다. 중재 제어는 시스템 운용을 총괄하는 모듈로서 다음 3가지 기술적 고려가 중요하다. 1) 프로세서 동기화, 2) 상호 배제(공유 자원 동시 접근 금지, 교착상태 회피), 3) 시스템 가용성. 대부분의 자동차 제어 임베디드 시스템에서 중재 제어는 시나리오나 조건, Truth table 기반으로 제어하는 하는 것이 일반적이다. 이는 예측 못한 시나리오나 케이스, 그리고 동작 타이밍에 상당한 취약점을 가질 수 있다. 반면 세마포어는 공유 리소스의 동시 접근 및 교착상태를 피하기 위해 사용되는 알고리즘으로 Critical section(임계 구역)을 이용하여 변수를 공유함으로써 동시 접근 가능한 제어기 시스템의 동기화 문제

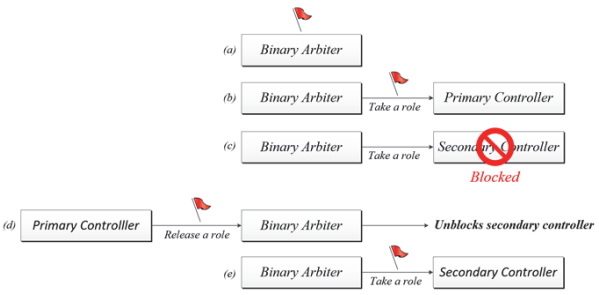


Fig. 5 Role decision-making scenario with binary semaphore
(a) Binary arbiter initializes single flag
(b) Primary controller gets the shared resource
(c) Secondary controller try to get the shared resource, but blocked
(d) Primary controller get done with the shared resource
(e) Secondary controller gets the shared resource

를 해결할 수 있다.[6)] 바이너리 세마포어는 0 or 1 상태만 갖는 것으로 0은 사용 불가능, 1은 사용 가능한 상태이다. 이는 두 개의 동일한 제어기 상호 배제 상태가 보장되어야 하고 어느 제어기도 Role을 가져가지 못하는 교착상태로 빠져서도 안된다.

Fig. 5는 이중화 시스템에서 바이너리 세마포어 알고리즘을 적용하여 공유 리소스를 충돌없이 획득(Take) 하고 반환(Release)하는 개념 흐름도를 보여준다. SbW 이중화 시스템의 경우 공유 자원인 시스템 운용 제어권은 오직 한 제어기에만 할당되어야 한다. 바이너리 중재 제어 모듈이 제어기-1에 리소스 플래그를 할당하면 다른 제어기가 제어기-1에서 플래그를 해제할 때까지 차단되어야 한다.[7)] 허용할 수 없는 결과를 초래하는 시스템 결함이 감지되면 제어기-1에 할당된 리소스 플래그를 해제한다. Fig. 6은 세마포어 제어를 구현하기 위한 Flow chart를 보여주는 것으로 각 제어기는 초기화 이후 공유 리소스 데이터의 값을 동기화하고 동작 상태에 따라 공유 리소스는 Take( ) 하거나 Release( ) 하게 된다.

3.3 이중화 된 E/E 시스템의 상태 제어

Fig. 6에서 “초기화” 단계는 전원 공급, 시스템 진단 실행, 두 제어기 사이의 입력, 출력 및 시스템 상태를 동기화하는 순서로 시스템을 초기화한다. “종료” 단계는 소프트웨어 제어기 뿐 아니라 조향 시스템도 정상적으로 종료한다. 제어기-1, 2 섹션은 각 시스템 상태로 구성된다. 바이너리 중재 제어 모듈은 시스템 초기 시점에 제어기-1,2의 Active role을 결정한다. 제어기-1 시스템이 Active 상태로 Role 이 결정되어 제어하는 경우 제어기-2는 시스템 결함이 감지될 때까지 Active role을 받을 준비

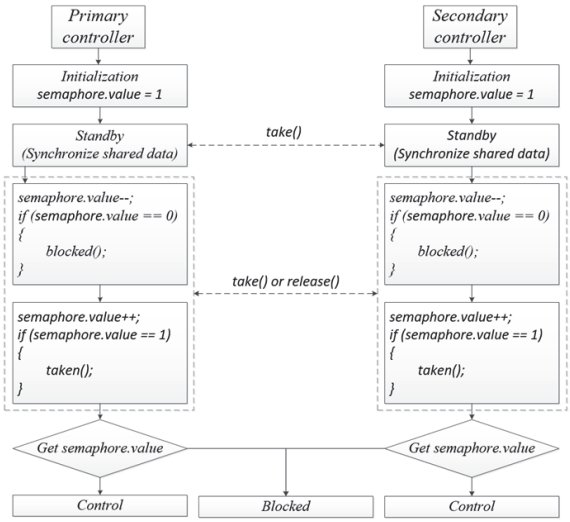


Fig. 6 Flow-chart for implementing source code with binary semaphore

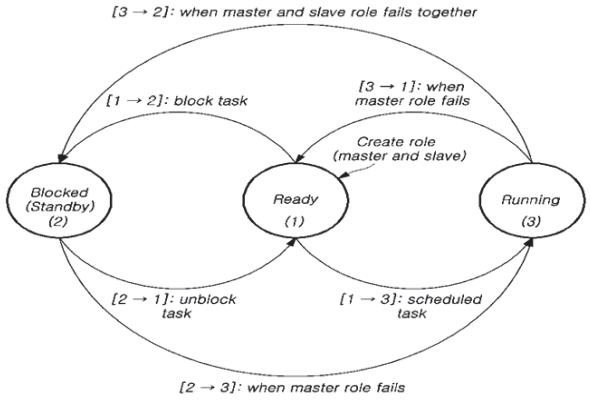


Fig. 7 State transition diagram in redundant control system

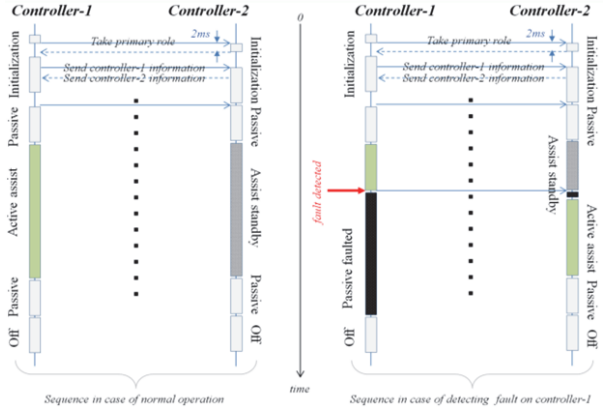


Fig. 8 System operational sequence in case of normal and a fault detected(at time domain)

상태인 Standby 모드에서 대기한다. 시스템 상태는 다음과 같이 정의된다.

- Binary Arbiter: ECU1, ECU2 제어기의 Role 결정
- Ready: 각 제어기의 제어 가능한 상태 결정 준비
- Blocked: 시스템 결함이 감지될 때 Backup 제어 Role을 받기 위한 대기 상태
- Active: 시스템을 제어하고 있는 상태
- Passive: 제어기가 시스템을 제어하지 않는 상태(전원 꺼짐 또는 결함 감지된 경우)

Fig. 8은 시스템 전원을 켠 후 두 제어기 사이의 초기화부터 종료까지 기본 동작 순서를 보여준다. 개별 제어기는 초기화 섹션에서 상호 배제를 보장하기 위해 바이너리 중재 제어 모듈을 통해 Role을 요청하고 결정한다. 또한 초기화 후, 각 제어기의 시스템 상태, 현재 제어 상태 모드 및 두 제어기 사이의 결함 상태를 포함한 각 제어기의 모든 정보를 IMC CAN, Dual CAN bus를 통해 주기적으로 공유한다. Fig. 8은 바이너리 중재 제어 모듈에 의해 제어되는 시퀀스 다이어그램 예로서 정상 동작 시퀀스에서 시스템 운용은 제어기-1은 Active 상태를 취하고 다른 제어기는 Standby 모드에서 대기하게 되고, 제어기-1의 결함 발생 시에는 FTTI 요구에 따라 제어기-2(Backup)로 전환하여 시스템 성능을 지속하는 것을 보여준다.

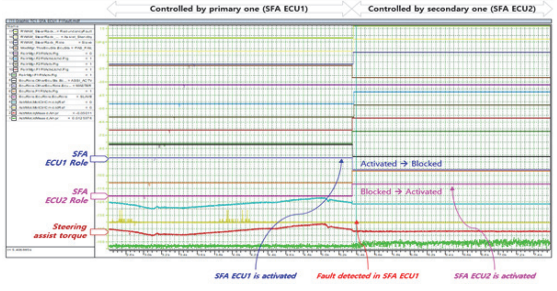
4. 연구(실험) 결과

본 4절에서는 차량과 벤치 테스트 환경 조건에서 고장 주입 방법을 이용하여 이중화 된 SbW E/E 제어 시스템 아키텍처의 가용성, 안전성에 대한 평가 결과를 보여준다. Table 2는 SbW 시스템의 기능 안전 목표를 기술한 것으로서 분석을 통해 시스템 신뢰성 평가를 위한 시험 시나리오를 도출하여 검증을 수행했으며 이를 기반으로 SbW 시스템 이중화 아키텍처의 가용성과 안전성을 입증했다. 기존 대부분의 연구에서 보여준 SbW 시스템의 이중화 전략이나 컨셉은 차량이나 시스템 파라미터를 이용한 동적 추정 모델로서 기능 안전을 제외한 기능 설계에 집중하고 있다.[11] 본 연구에서는 SbW 시스템의 HARA 분석을 토대로 기능 안전 목표를 수립하고 HMT를 통해 얻은 FTTI와 Lateral-g를 기반으로 본 연구에서 제안하는 이중화 시스템 모델의 안전성을 실험적으로 평가했다. 이는 고장 발생 시 운전자에게 어떠한 편차없이 지속적으로 시스템 성능이나 기능을 제공할 수 있는지를 검증하는 것으로 시스템의 안전성과 신뢰성을 보여준다.

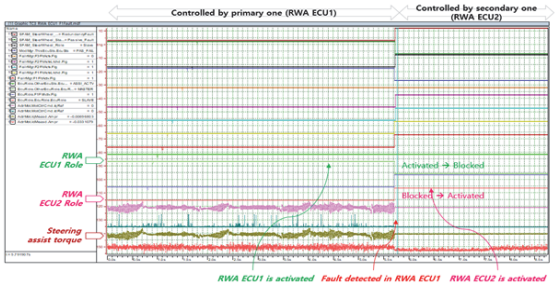
Figs. 9, 10은 E/E 이중화 시스템 아키텍처의 신뢰성테

Table 2 Safety goals of steer-by-wire system

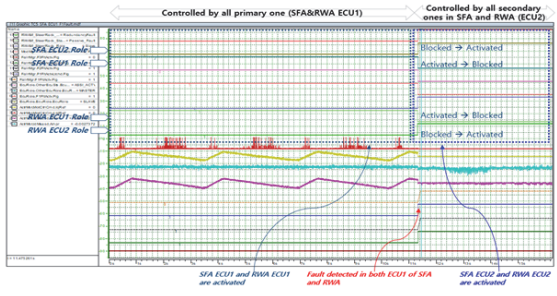
Id	Safety goals	ASIL	Safe state
SG-1	Insufficient control of vehicle lateral control in the system shall be prevented	C	Normal (w/o deviation)
SG-2	Loss of vehicle lateral control in the system shall be prevented	D	Normal (w/o deviation)
SG-3	Unintended vehicle lateral motion in the system shall be prevented	D	Normal (w/o deviation)
SG-4	Incorrect steering feedback in the system shall be prevented.	C	Normal (w/o deviation)
SG-5	Inability to allow driver to take over in autonomous mode shall be prevented.	D	Normal (w/o deviation)



(1) In case of a fault detected in primary controller of SFA



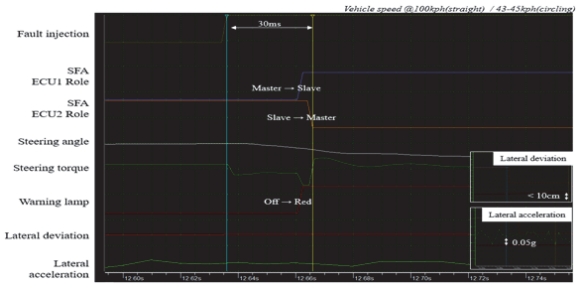
(2) In case of a fault detected in primary controllers of RWA



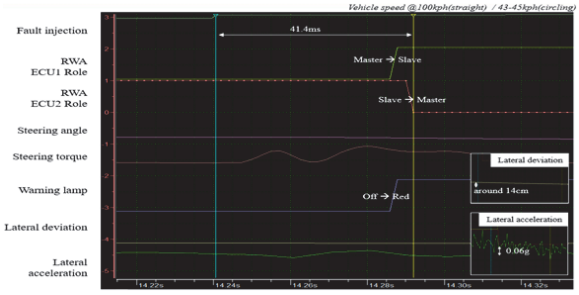
(3) In case of a fault detected in primary controllers of both SFA and RWA

Fig. 9 Test result on scenarios of system fail operation in redundant environments

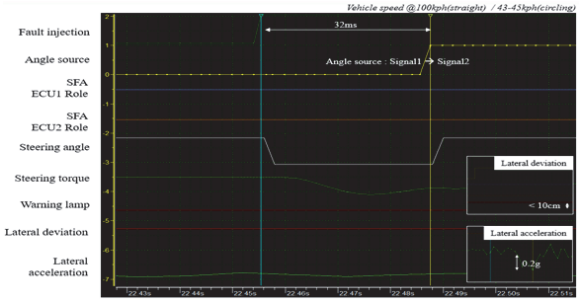
스트를 위해 차량과 SbW 시스템 벤치 테스트 실험 환경을 구성하여 검증한다. Fig. 9는 시스템 벤치 테스트 검증을 위해 센서, Power Pack, CAN analyzer, 고장 주입 유닛으로 구성하여 Fail operation에 대한 3가지 테스트 시나



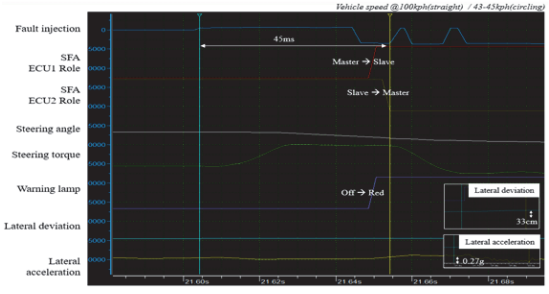
(1) The motor position sensor fault detected in SFA ECU1



(2) The motor position sensor fault detected in RWA ECU1



(3) The steering angle fault detected in SFA ECU1



(4) The motor position sensor fault detected in SFA ECU1

Fig. 10 Safety validation result on scenarios of system fail operation in vehicle environments

리오에 대한 결과를 보여주는 것으로 Fig. 9(1), (2)는 각 SFA, RWA 제어기의 ECU-1에서 정상 제어 중 결함이 감지된 경우로 ECU-1의 제어권은 Blocked 상태가 되고 ECU-2에게 시스템 제어권이 전환되는 것을 보여준다. Fig. 9(3)는 SFA와 RWA 제어기의 ECU-1에서 동시에 결함이 감지되었을 때 각 제어기의 제어권이 ECU-2로 천이 되는 결과를 보여주는 것으로 SbW 시스템은 동작 중 결함 발견 시에도 성능 제약없이 계속해서 정상적으로 시스템 기능을 제공할 수 있다는 것을 실험적으로 입증했다. 다음 Fig. 10은 실제 차량에서 실시한 시스템의 안전성 검증 결과를 보여주는 것으로 100 Kph 직진 주행 중 SbW 시스템에 강제 고장을 주입하여 시스템의 고장 운용 성능에 대한 평가를 수행한다. Fig. 10(1)은 직진 100 Kph 주행과 43 ~ 45 Kph 선회 주행 조건에서 각각 SFA ECU-1 토크센서 고장 주입에 대한 결과로 FTTI 45 ms 이내 고장 검출과 Role 천이까지 수행하여 운전자에게 위험없이 정상적인 조향 어시스트를 지속적으로 제공하는 것을 보여준다. 그 외 나머지 Fig. 10(2), (3), (4) 테스트 시나리오도 동일 주행 조건에서 각각 RWA ECU-1 모터위치센서 고장, SFA ECU-1 조향각 고장, SFA ECU-1 모터위치센서 고장 주입에 대한 실험 결과들로 기능 안전 요구에 부합하는 결과를 보여주고 있으며, 이 같은 SbW 시스템의 기능 안전에 대한 평가는 HMT 실험 결과에서 얻은 FTTI와 Lateral-g deviation을 기준으로 판단된다.

5. 결 론

앞서 언급된 바와 같이 조향, 제동 시스템과 같이 차량 안전 관련 중요 제품들의 E/E 시스템 이중화 아키텍처 전략은 시스템의 가용성을 높여 운전자에게 가할 수 있는 치명적인 위험을 줄이고 시스템의 안전성을 향상시킬 수 있도록 도와준다. 본 연구에서는 두 개의 동일한 제어기가 구성된 이중화 된 SbW E/E 시스템 동작 운용의 신뢰성 향상을 위해 바이너리 세마포어 방식을 이용한 상호 배제와 교착 상태 보호 가능한 중재 제어 방법을 제안, 분석하고 평가했다. 또한 ISO26262에 따라 SbW 시스템의 기능 안전 목표를 수립하고, E/E 이중화 제어 시스템 아키텍처의 안전성을 평가하고 검증했다. 향후 연구에서는 본 성과를 기반으로 차량 수준의 시스템 응답성, IMC CAN 통신 시간, 전환 수행 시간, FTTI 요소들의 최적화 설계를 통해 SbW E/E 이중화 제어 시스템의 운용 최적화에 대한 연구를 수행하고자 한다.

후 기

본 논문은 HL 만도 SW Campus와 조향 사업부 R&D 센터의 연구지원 아래 수행되었다.

References

1) A. D. Dominguez-Garcia, J. G. Kassakian and J. E. Schindall, “A Backup System for Automotive Steer-By-Wire, Actuated by Selective Braking,” IEEE 35th Annual Power Electronics Specialists Conference, Vol.1, pp.383-388, 2004.
2) R. P. Patankar, “A Model for Fault-tolerant Networked Control System Using TTP/C Communication,” IEEE Transactions on Vehicular Technology, Vol.53, No.5, pp.1461-1467, 2004.
3) J. H. Lee, H. T. Moon and J. Y. Yoo, “Current Sensorless drive Method for Electric Power Steering,” Int. J. Automotive Technology, Vol.13, No.7, pp.1141-1147, 2012.
4) X. Ji, J. Ge and H. Tian, “Reliability Improvement of Electric Power Steering System Based on ISO 26262,” International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE), pp.125-129, 2013.
5) W. Harter, W. Pfeiffer, P. Dominke, G. Ruck and P. Blessing, Future Electrical Steering Systems: Realizations with Safety Requirements, No. 2000-01-0822. SAE Technical Paper, 2000.
6) J. Guldner and T. Irina, “Comparison of Redundancy Structures for Safety Relevant Automotive Control Systems,” European Control Conference(ECC), pp.2818-2823, 1999.
7) F. Cicirelli and N. Libero, “Modelling and Verification of Starvation-Free Mutual Exclusion Algorithms Based on Weak Semaphores,” Federated Conference on Computer Science and Information Systems (FedCSIS, pp.773-779, 2015.
8) ISO, ISO 26262: Road Vehicles - Functional Safety, International Standard ISO/FDIS 26262, 2011.
9) H. Hu, G. Wang, L. Zeng, Y. Li, A. Zhang and J. Zhou, “Dual Network Redundancy Control and Arbitration Strategy Research in HVDC Control and Protect System,” IEEE 5th International Conference on Electronics Information and Emergency Communication, pp.116-121, 2015.
10) J. S. Kim, W. G. Hwang and W. S. Lee, “Development of a Fault-tolerant Steer-by-Wire Control System,” Transactions of KSAE, Vol.14, No.5, pp.1-8, 2006.

11) K. Polmans, “Torque Vectoring as Redundant Steering for Automated Driving or Steer-By-Wire,” 5th International Munich Chassis Symposium, Springer Vieweg, Wiesbaden, 2014.

12) D. S. Kim, J. H. Lee and J. Namgung, “A Study on Arbitration Control Method of Steer-by-Wire System in Dual Redundancy Environments,” KSAE Spring Conference Proceedings, pp.278-285, 2021.