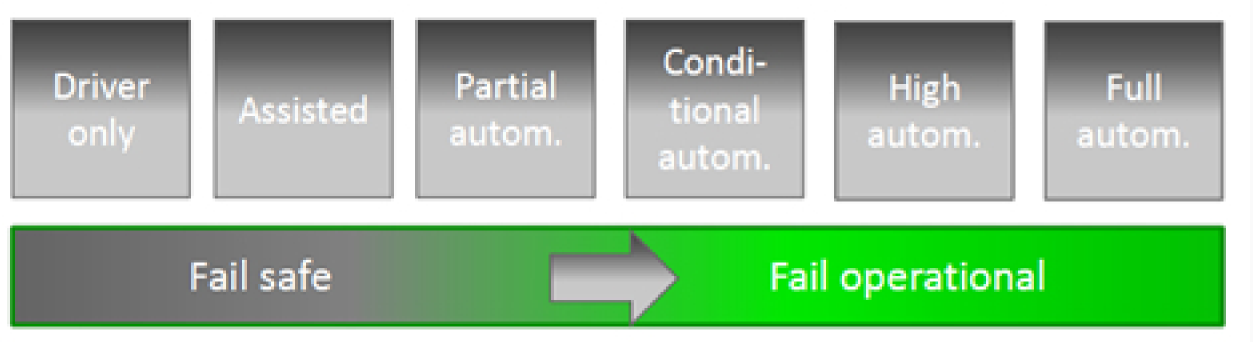
자율주행 Fail operational safety architcture

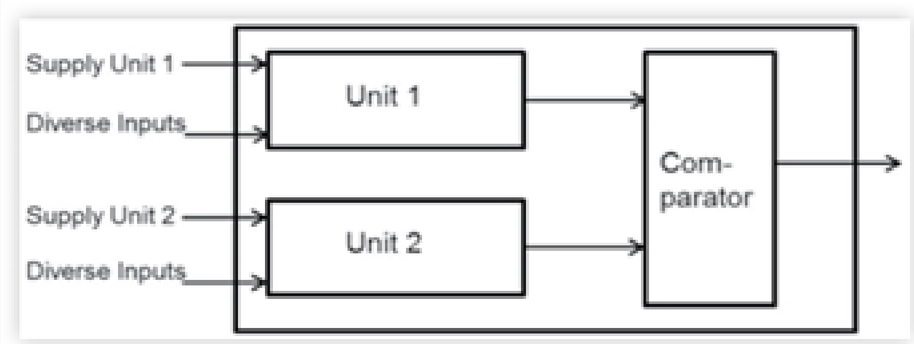
“ 자율주행 시스템은 차량 고장 발생 시 주로 Switch off를 통해 안전상태로 전환하는 전통적인 ISO26262에서의 Fail-Safe 보다 시스템의 현 기능을 계속 작동하기 위한 Fail Operational 안전 아키텍처가 요구됩니다. ”

- 자율주행 레벨에 따른 Fail operational 안전 아키텍처 적용

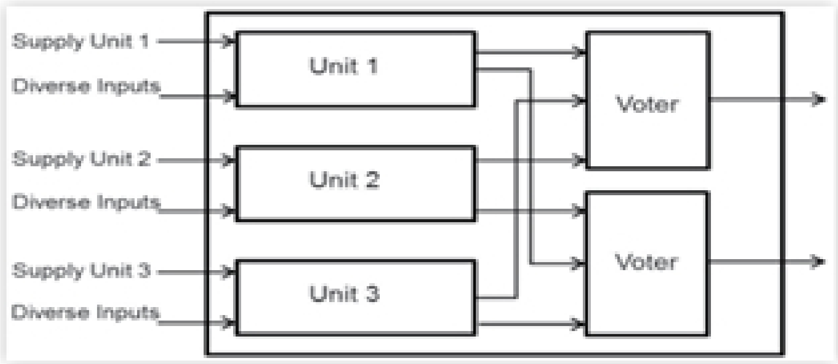


Fail operational 안전 아키텍처는 기본적으로 (Dirverse) Redundancy를 사용하며 다음과 같은 Fail operational 원칙을 바탕으로 구성될 수 있습니다.

- 1oo2 Fail operational safety architecture

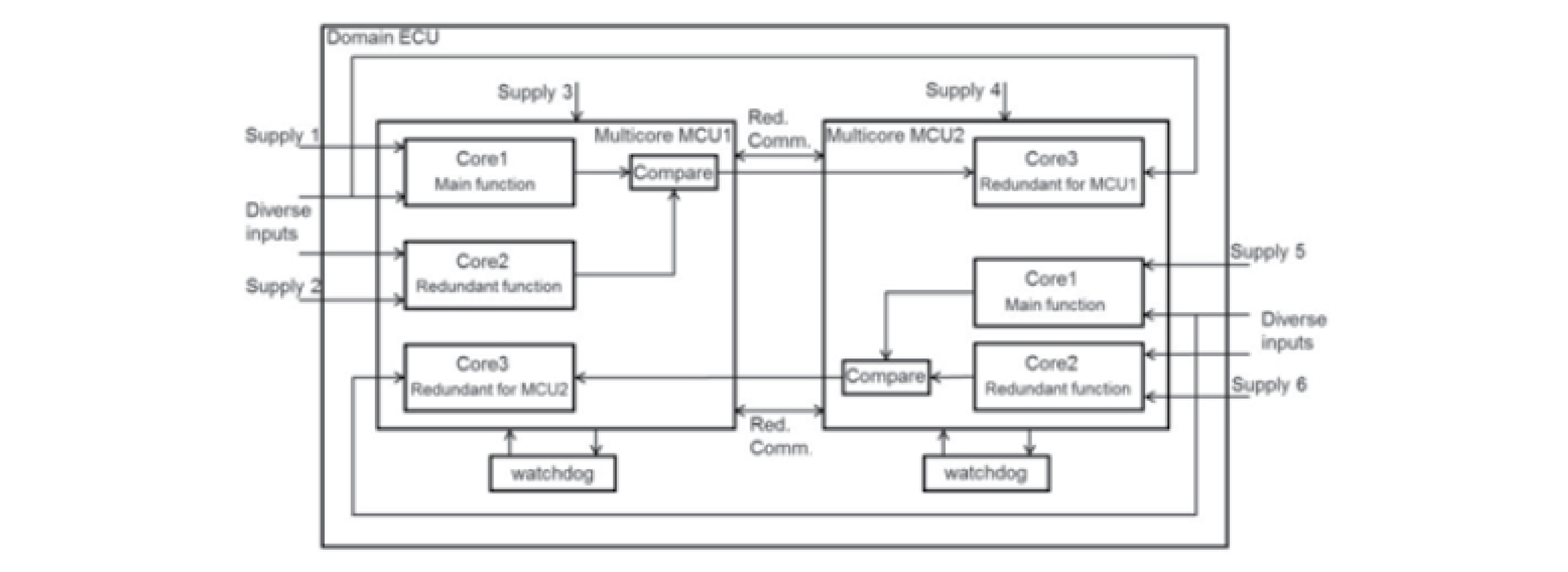


- 2oo3 Fail operational safety architecture



특히, Fail operational 안전 아키텍처는 자율주행 레벨에 따라 전반적인 전략이 결정되어야 합니다. 예를 들어 SAE 자율 주행 레벨 3는 시스템 요청 시 차량 제어권을 운전자가 받을 수 있을 수 있는 반면, SAE 자율 주행 레벨 4 이상의 경우 운전자 개입 없이 시스템 스스로 DDT (DYNAMIC DRIVING TASK) FALLBACK을 할 수 있도록 설계되어야 합니다.

다음 그림은 자율주행 레벨 3를 위한 Failure Operational Architecture에 대한 예시로써 센서 고장 발생 시 MCU 상의 별도 코어에서 작동하는 FALLBACK을 통해 운전자에게 차량 제어권을 이양할 수 있도록 아키텍처가 설계되어 있음을 알 수 있습니다.



(출처: Sari, B. and Reuss, H.-C., “Fail-Operational Safety Architecture for ADAS Systems Considering Domain ECUs,” SAE Technical Paper 2018-01-1069, 2018, doi:10.4271/2018-01-1069.)