안전이란? 허용 가능하지 않은 리스크가 없는 상태?  
기능 안전이란? 전기전자 시스템(모니터링 센서 및 제어 SW)에서 오동작을 야기하는 hazard (Harm의 원인이 되는 잠재적인 요인들) / 허용할 수 없는 리스크가 없는 상태

Risk란? 잠재적인 문제, hazard가 accident로 이어질 가능성과 심각도

HARA : Hazard Analysis Risk Assessment  
TARA : Threat -, 사이버보안에서.

안전 무결성 요구사항: 시스템마다 만족해야 하는 안전 관련 등급이 있는데, 그 등급에 따라 만족해야 하는 안전 기능의 품질이 결정된다.

QM (in ASIL 등급): 허용할 수 있는 리스크.  
A~D를 QM으로 최대한 낮추기 위해 두가지 요구사항, 안전 기능 요구사항과 안전 무결성 요구사항을 충족시켜야 한다. 안전 기능 요구사항은 곧 결함 감지와 결함 조치가 해당된다. 무결성은 안전 기능 요구사항의 품질을 높이는 것.

안전 목표는 추상적인 목표일 뿐, 구체적인 해결 방법은 요구사항에 기재.

시스템의 전제 최종 ASIL 등급은 각 Hazardous Events들의 등급 중 가장 높은 등급이 된다.  
예를 들어, 스마트키 같은 경우 기능 중에 스티어링 라킹하는 기능이 있는데 나머지 기능은 다 QM인데, 이 라킹 기능이 D 등급이 돼서 최종 D 등급이 되는 경우도 있다.

특별히 소프트웨어 요구사항에 대한 공학적 접근을 다루는 요구 공학이라는 학문도 있다.  
요구사항 개발 프로세스 : 도출 -> 분석 -> 명세 -> 검증  
도출 : 특히 암묵적 요구사항을 찾아내야 한다. 잠재적인 후보 요구사항도 도출한다.   
분석 : 개발자 관점에서, 요구사항 분석해서 우선순위 결정. 우선순위는 또 고객의 관점에서., 타당성도 고려. 리스크 발견 -> 계획 단계에서 고려.  
명세 : 요구사항 명세 방법 (양식, 기준) 선정하여 품질을 높인다.  
검증 : 헐 검증 기준도 정해야된대 어쩐지