

휴먼에러와 안전 사고(incident)

- 휴먼에러에 의한 사고 %
- 대부분 사고는 여러 복합 요인에 의해 발생
- 불안정한 행동 vs 불안정한 상태
- 사고 분석에서 어떤 관점(perspective)을 취할 것인가? The broad or the narrow?
 - 항공기 사고의 파일럿의 실수 부각 (narrow)
 - 항공기 설계 상의 오류와 상황 (broad)

휴먼에러 대책

- 휴먼에러는 어쩔 수 없는 것이다 (x)
- 휴먼에러의 결과와 가능성을 줄일 수 있다 (O)
 - 올바른 인사선발
 - 적절한
 - 안전에 대한 동기부여
 - 적절한 체크리스트 제공
 - 인간을 고려한 시스템, 절차, 환경 설계

휴먼에러 예방대책

1. 일반적 휴먼에러 대책

- 작업장에 적합한 종업원 선발
- 작업 수행에 필요한 교육과 훈련 실시
- 안전행동을 위한 동기 부여
- 인간을 고려한 시스템과 작업 설계

2. 시스템 설계 시 휴먼에러 대책

휴먼에러에 대한 디자인 원칙

1. 에러 제거 디자인(error exclusion design)
 - 에러 발생을 근본적으로 하게 설계
 2. 에러 예방 디자인 (error prevention design)
 - 에러 발생이 어렵도록 설계
 3. 안전장치의 장착(provision of safety device)
 - 에러 발생 보다 그 결과를 최소화하기 위한 설계
 4. 경보장치의 부착(provision of warning devices)
 - 안전설계 원칙이 부족하여 사고 발생의 위험이 있을 때에는 사고 시 이에 대한 위험을 알려주는 경보장치 등을 부착하여 이에 대비하게 함
 - 화재경보 장치나 자동차에서의 후방거리 안내 표시등
 5. 특수 절차서의 제공(provision of special procedure)
 - 사고 발생 시의 대처 요령이나, 안전한 사용을 위한 사용자 매뉴얼 등
-

휴먼에러에 대한 디자인원칙

- 오류의 원인을 이해하고 그 원인을 최소화
- 오류 수정들을 위해 행동을 역으로 하는 것(Undo)이 가능하도록 하라. 그것이 불가능하면 오류 발생 시 조작이 불가능하도록 하라
- 발생한 오류를 발견하기 쉽고 고치기 쉽게 하라

인간공학적 디자인원칙

□ 디자인

- 설계 단계에서 사용하는 재료나 기계 작동 메커니즘 등 모든 면에서 휴먼에러 요소를 근원적으로 제거하도록 하는 디자인 원칙
- 유아용 완구의 표면을 칠하는 도료는 위험한 화학물질 일 수 있다. 이런 경우 도료를 먹어도 무해한 재료로 바꾸어 설계

인간공학적 디자인원칙

□ 디자인

- 근원적으로 에러를 100% 막는다는 것은 실제로 매우 힘들 수 있고, 경제성 때문에 그렇게 할 수 없는 경우

- 가능한 에러 발생 확률을 최대한 낮추어 주는 설계

- 신체적 조건이나 정신적 능력이 낮은 사용자라 하더라도 사고를 낼 확률을 낮게 설계해 주는 것을 에러 예방 디자인

- 풀-푸르프(fool proof) 디자인

- 세제나 약 병의 뚜껑을 열기 위해서는 힘을 아래 방향으로 가해 돌려야 함

- 컴퓨터와 모니터를 연결하는 케이블과 같이 전자기기의 케이블에서 꽂는 방향이 잘못 되면 연결이 안 되고, 오직 정확한 방향으로만 체결이 되게 하는 것
-

인간공학적 디자인원칙

- 원칙
 - Good mapping (대응의 원칙)
 - Visibility (가시성의 원칙)
 - Feed back (피드백의 원칙)
 - Restriction (사용의 제약)



인간공학적 디자인원칙

□ 안전장치의 장착

■ Fail safe 디자인

- 사용자가 휴먼에러 등을 범하더라도 그것이 부상 등 재해로 이어지지 않도록 안전장치의 장착을 통해 사고를 예방

■

- Redundant system (중복설계)

- 비행기 엔진을 2 대 이상으로 설계

- Standby system (대기 시스템 설계)

- 수술 중 정전(fail)에 대비해 병원에 자가 발전기(safe)를 대기

- 자동차의 보조 바퀴

- Error recovery (에러 복구) 혹은 고장 난 시스템이 더 이상 작동하지 않게 하는 방식

- 에러 복구 가능한 시스템의 예: 윈도우 시스템의 휴지통 기능

- 고장 난 시스템이 더 이상 작동하지 않도록 하는 예: 전기 히터는 넘어지는 사고가 발생하면 위치 센서가 작동하여 전원이 자동으로 차단

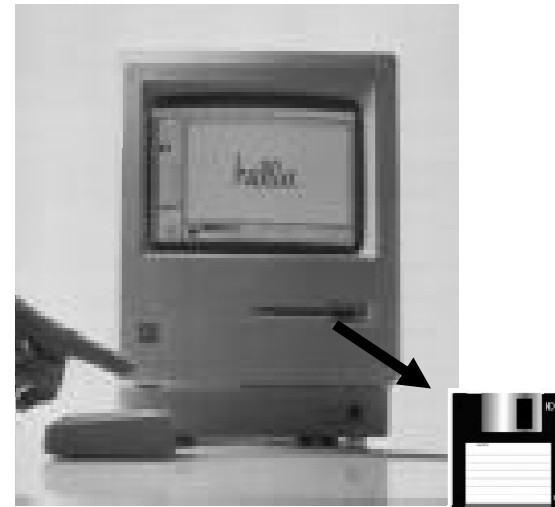
안전을 위한 설계

□ 설계원칙



넘어지면 자동으로
전원이 차단

□ Fool-Proof 설계원칙

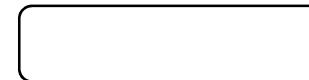


전원을 끄면 자동으로
디스켓이 추출

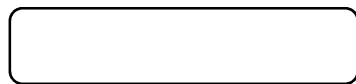
부품중복설계와 대기부품설계



중복 설계(예)
Airplane Engines



에러복구 체계



1998년 12월4일 나이키 미사일 오발사고
(발사한 미사일에 표적이 할당되지 않으면 이 미
사일은 자폭하도록 만들어졌다).

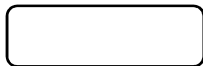
휴먼에러를 막는 디자인

- 강제적 기능(forcing function)의 설치- 물리적 제약
 - 설계단계에서 휴먼에러의 예방을 위해 위험한 시스템이나 시스템의 위험한 부분의 접근을 차단할 필요
 - 맞잠금(interlock)장치
 - 동작되는 기계 장치 등에 대해 접근이 이루어지면 자동으로 동작을 멈추도록 설계한 잠금장치
 - 세탁기의 도어 open시 회전 멈춤
 - 안잠금(lockin)장치
 - 시스템의 안 쪽에서 접근을 방지하는 장치
 - 전기 압력 밥솥
 - 컴퓨터 시스템의 종료 전 파일 저장 확인
 - - 시스템의 보수 등의 작업을 실시할 때 그 사실을 모르는 사람이 급작스레 기계 장치를 동작시키거나 에너지 분출을 막기 위해 기계 조작 장치 등을 외부에서 잠그는 것
 - 정비 중인 기계 표시
 - 지하 층으로 통하는 문의 출입 제한

lock-in/lock-out/interlock



고압의 증기 분출 방지



위험장소 접근방지



세탁기 회전 정지

