시스템 안전 분석

-위험 및 운용성 분석 (Hazard and Operability Analysis: HAZOP)-

충주대학교 안전공학과
박 정 철

HAZOP 개요

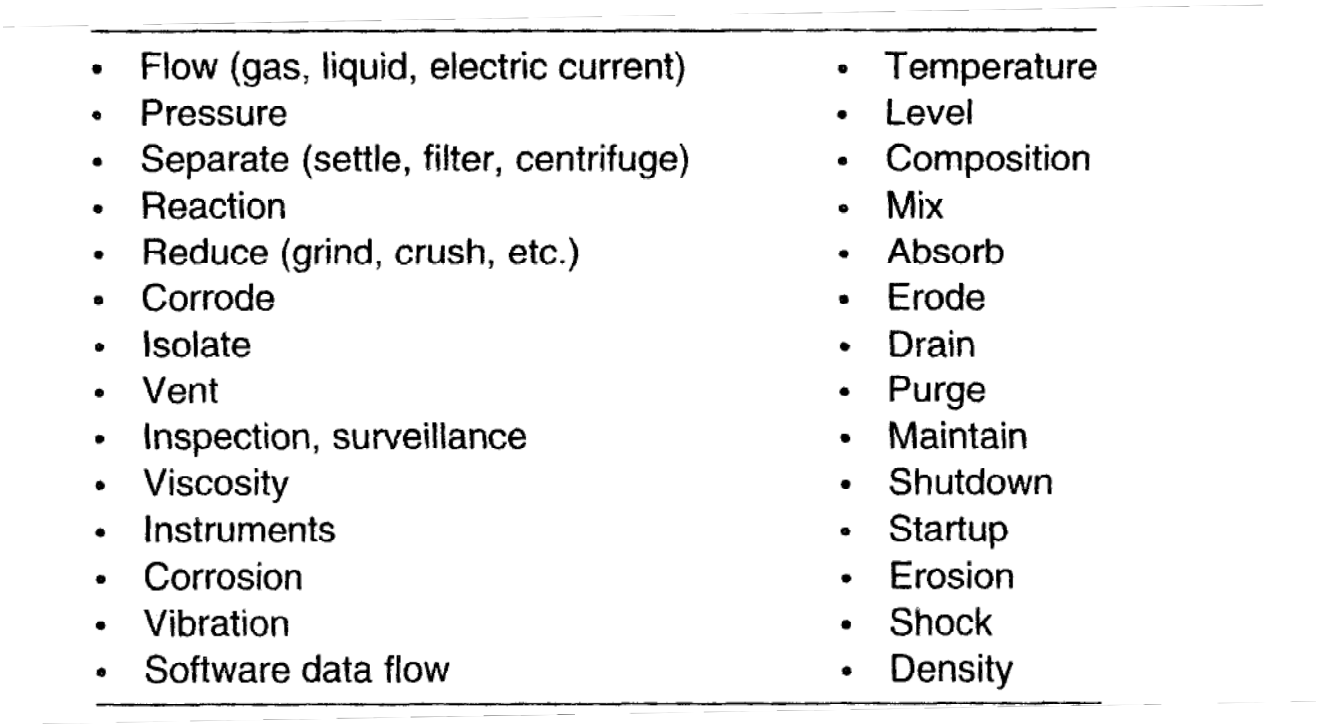
- Hazard and Operability Analysis (or Studies)
  - 시스템의 위험 파악 및 운용적 측면 분석 (효율화)
  - 다양한 분야의 전문가(+ 리더)로 구성된 팀의 브레인스토밍
  - Guide word (more, no, less 등의 형용사)와 프로세스/시스템 조건(speed, flow, pressure 등) 결합
- 목적
  - Guide word를 활용해 시스템 운용상의 의도에서 벗어난 잠재적 이탈 상태 파악
  - 다양한 레벨의 각종 시스템에 적용 가능 (서브시스템, 어셈블리, 컴포넌트, 소프트웨어, 절차, 환경, 인적 오류 등)
- 역사
  - 1970년대 초반 Institute of Chemical Industry (ICI) 화학공정 안전 분석
  - Flixborough 화학공장 폭발 사고 이후 정유산업, 식품산업, 음료산업 등으로 전파
- 시점
  - 사전 설계 및 상세 설계 단계
- 대체 기법
  - PHA, SSHA

HAZOP 방법

- Guide word (가이드 워드) + System parameter (시스템 파라미터) = Deviation (이상)
  - Ex. 발열반응이 일어나는 화학 공정에서
    - More + reactant = 온도 급상승
    - 무의미한 조합이 있을 수 있음
      - No + temperature
      - Reverse + pressure
- Design representation
  - 도면, 구조, 블록 다이어그램, 기능 흐름도, 데이터 흐름도 등

System parameter

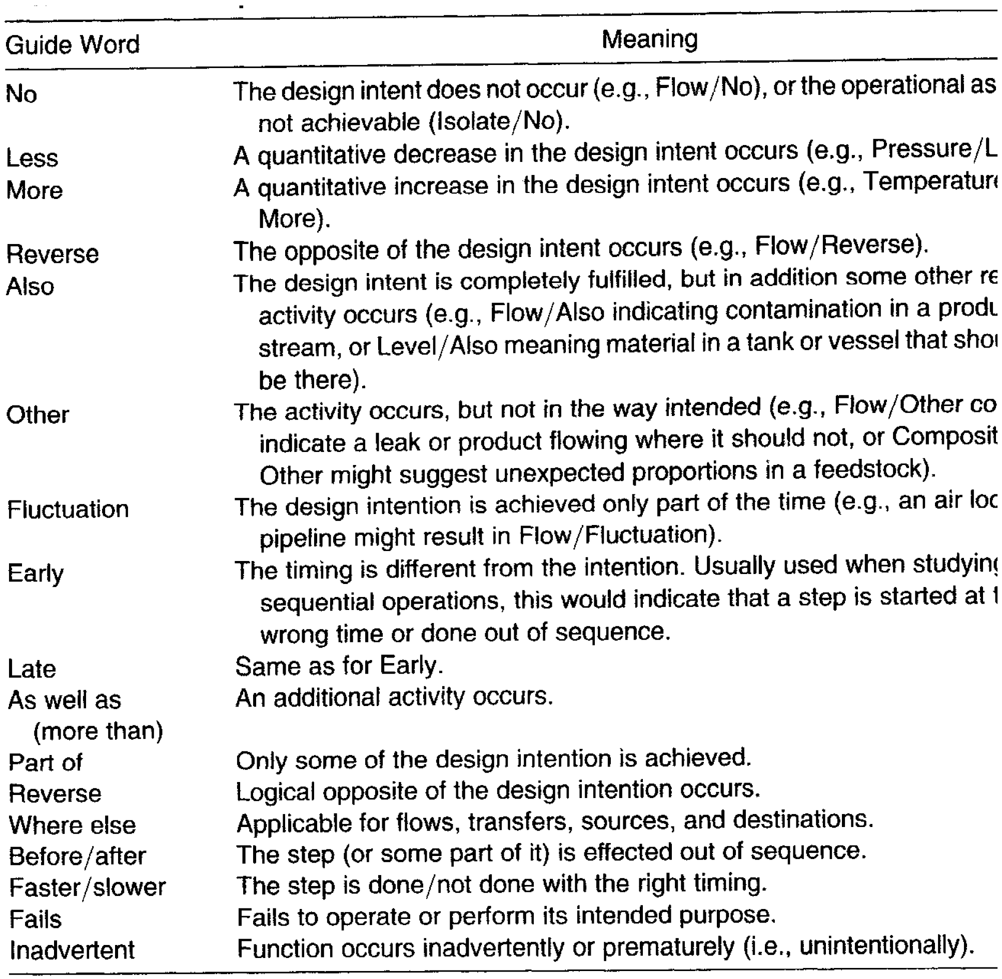
- System parameter
  - 공장, 공정, 시스템 등의 가변적 파라미터나 특징 (반응물, 반응 순서, 온도, 압력, 흐름, 단계 등)



- Flow (gas, liquid, electric current)
- Pressure
- Separate (settle, filter, centrifuge)
- Reaction
- Reduce (grind, crush, etc.)
- Corrode
- Isolate
- Vent
- Inspection, surveillance
- Viscosity
- Instruments
- Corrosion
- Vibration
- Software data flow
- Temperature
- Level
- Composition
- Mix
- Absorb
- Erode
- Drain
- Purge
- Maintain
- Shutdown
- Startup
- Erosion
- Shock
- Density

Guide word

- Guide word
  - 시스템의 비정상 상태에 대한 아이디어를 얻기 위해 사용되는 수식어



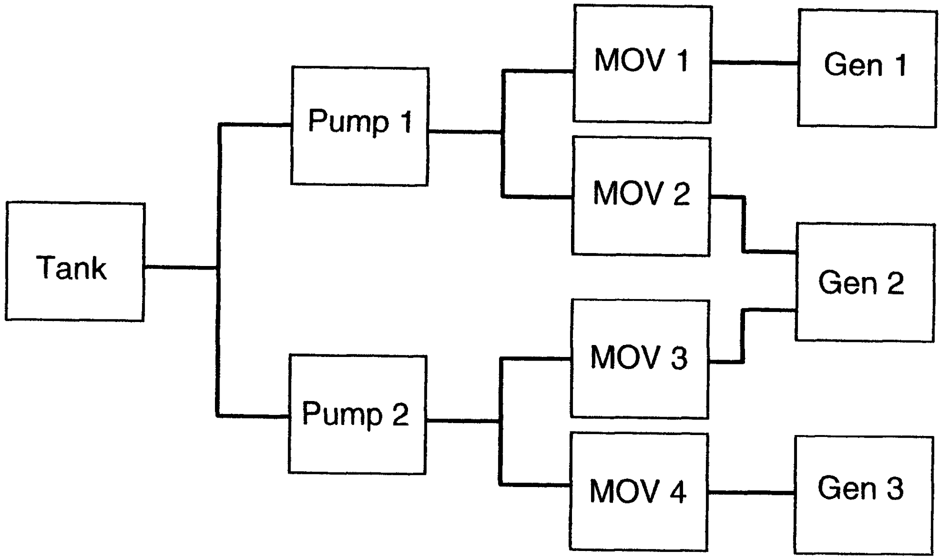
	Guide Word	Meaning
부재	No	The design intent does not occur (e.g., Flow/No), or the operational as not achievable (Isolate/No).
부족	Less	A quantitative decrease in the design intent occurs (e.g., Pressure/L
과다	More	A quantitative increase in the design intent occurs (e.g., Temperatur More).
역	Reverse	The opposite of the design intent occurs (e.g., Flow/Reverse).
부가	Also	The design intent is completely fulfilled, but in addition some other re activity occurs (e.g., Flow/Also indicating contamination in a produ stream, or Level/Also meaning material in a tank or vessel that sho be there).
여타	Other	The activity occurs, but not in the way intended (e.g., Flow/Other co indicate a leak or product flowing where it should not, or Composit Other might suggest unexpected proportions in a feedstock).
유동	Fluctuation	The design intention is achieved only part of the time (e.g., an air loc pipeline might result in Flow/Fluctuation).
이름	Early	The timing is different from the intention. Usually used when studyin sequential operations, this would indicate that a step is started at t wrong time or done out of sequence.
늦음	Late	Same as for Early.
추가	As well as (more than)	An additional activity occurs.
부분	Part of	Only some of the design intention is achieved.
	Reverse	Logical opposite of the design intention occurs.
다른곳	Where else	Applicable for flows, transfers, sources, and destinations.
다른순서	Before/after	The step (or some part of it) is effected out of sequence.
	Faster/slower	The step is done/not done with the right timing.
실패	Fails	Fails to operate or perform its intended purpose.
비의도	Inadvertent	Function occurs inadvertently or prematurely (i.e., unintentionally).

HAZOP 양식

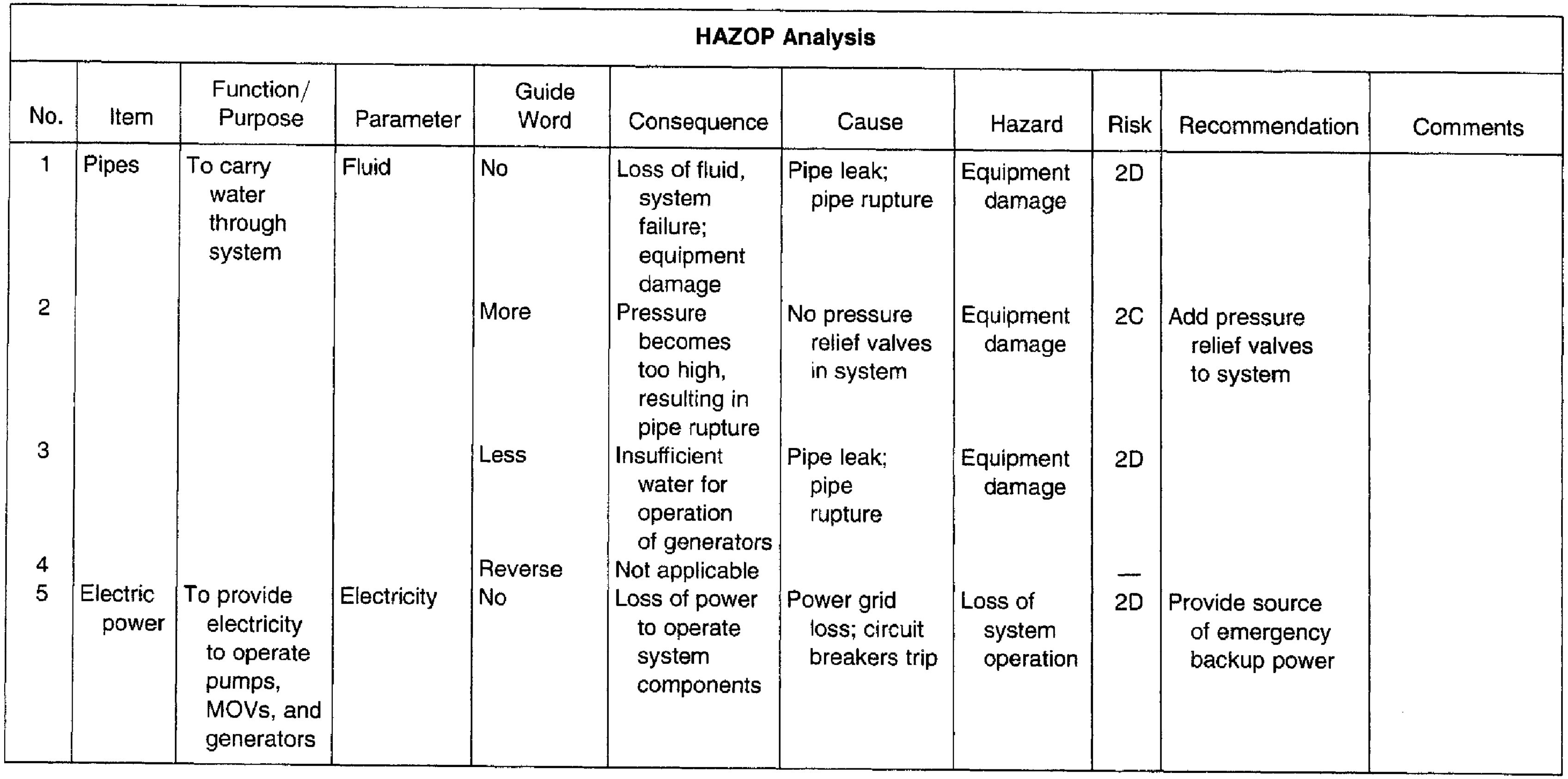
HAZOP Analysis										
번호	항목	기능/목적	파라미터	가이드워드	결과	원인	위험	리스크	조치	비고
①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪

HAZOP 예 – 스팀 발전 시스템

- 시스템 파라미터: 흐름, 압력, 온도, 전기, 스팀



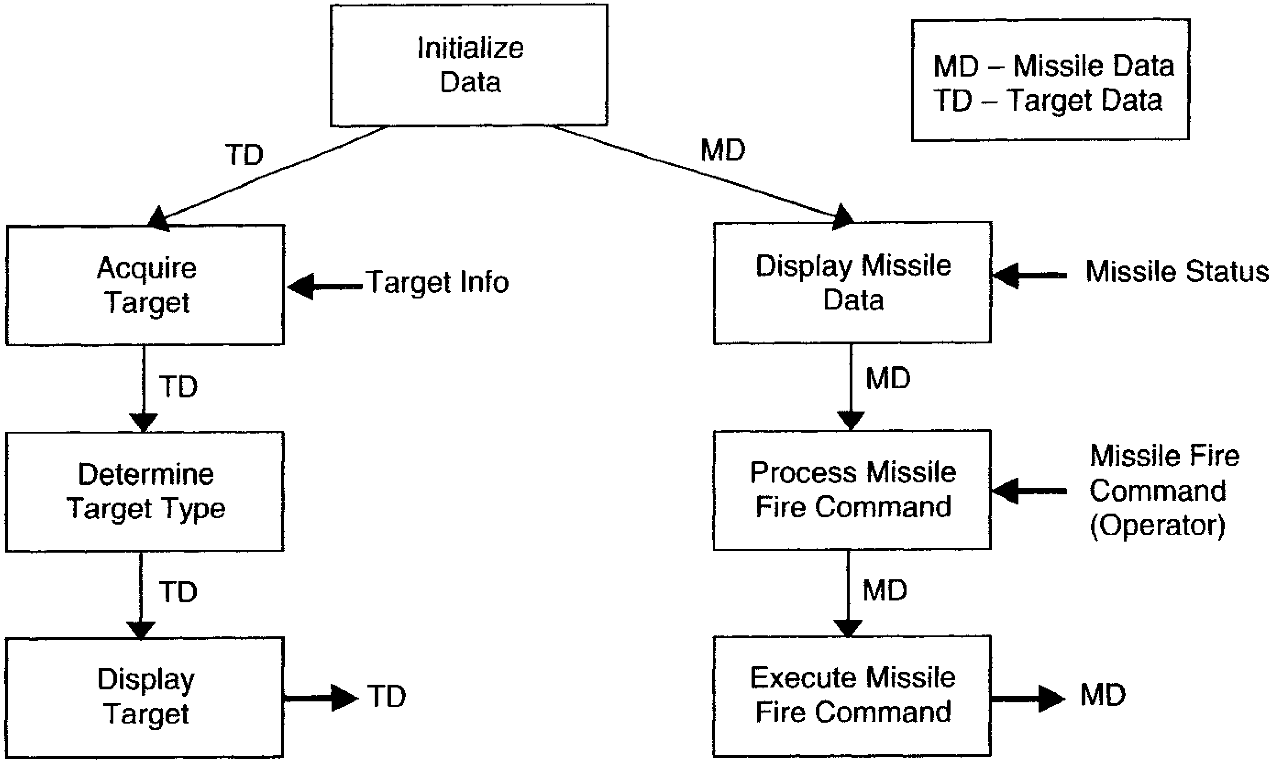
HAZOP 예 – 스팀 발전 시스템



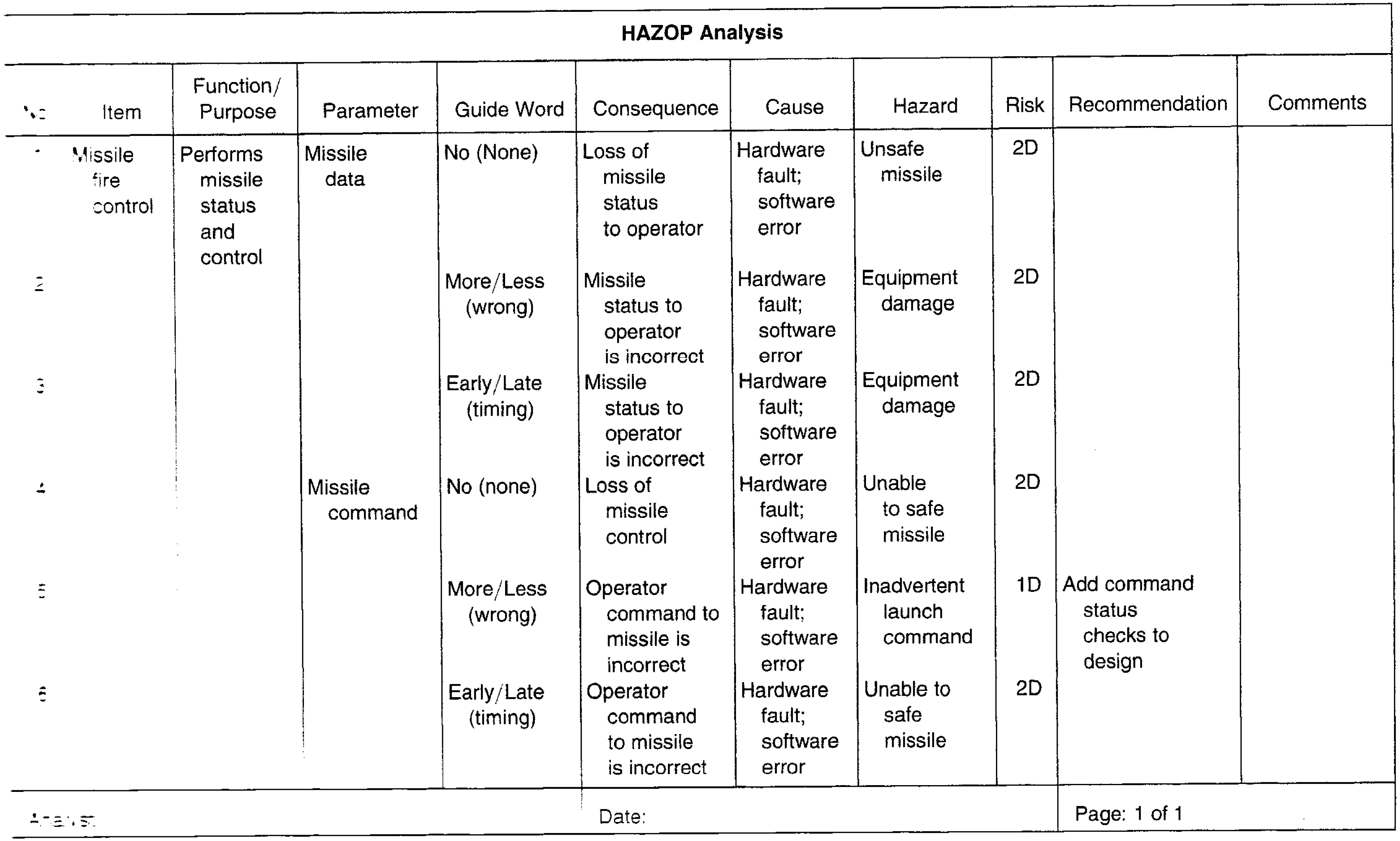
HAZOP Analysis

No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments
1	Pipes	To carry water through system	Fluid	No	Loss of fluid, system failure; equipment damage	Pipe leak; pipe rupture	Equipment damage	2D		
2				More	Pressure becomes too high, resulting in pipe rupture	No pressure relief valves in system	Equipment damage	2C	Add pressure relief valves to system	
3				Less	Insufficient water for operation of generators	Pipe leak; pipe rupture	Equipment damage	2D		
4				Reverse	Not applicable			—		
5	Electric power	To provide electricity to operate pumps, MOVs, and generators	Electricity	No	Loss of power to operate system components	Power grid loss; circuit breakers trip	Loss of system operation	2D	Provide source of emergency backup power	

HAZOP 예 – 미사일 발사 제어 소프트웨어



HAZOP 예 – 미사일 발사 제어 소프트웨어



HAZOP Analysis

No	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments
1	Missile fire control	Performs missile status and control	Missile data	No (None)	Loss of missile status to operator	Hardware fault; software error	Unsafe missile	2D		
2				More/Less (wrong)	Missile status to operator is incorrect	Hardware fault; software error	Equipment damage	2D		
3				Early/Late (timing)	Missile status to operator is incorrect	Hardware fault; software error	Equipment damage	2D		
4			Missile command	No (none)	Loss of missile control	Hardware fault; software error	Unable to safe missile	2D		
5				More/Less (wrong)	Operator command to missile is incorrect	Hardware fault; software error	Inadvertent launch command	1D	Add command status checks to design	
6				Early/Late (timing)	Operator command to missile is incorrect	Hardware fault; software error	Unable to safe missile	2D		

Analyst: Date: Page: 1 of 1