HAZARD ANALYSIS

Index

- Hazard analysis의 정의
- Hazard analysis의 필요성
- Development process와 hazard analysis
- Hazard analysis 기법 유형
- Hazard analysis 기법들
  - Fault tree analysis (FTA)
  - Failure mode and effects analysis (FMEA)
  - Hierarchically performed hazard origin and propagation studies (HiP-HOPS)
  - System theoretic process analysis (STPA)
  - Software system safety engineering process
- Issue

HAZARD ANALYSIS의 정의

Hazard analysis의 정의

- Accident
  - Any unplanned event or series of events that results in death, injury, or illness to personnel or damage to or loss of equipment or property. Accident is synonymous with mishap.
- Hazard
  - A condition that is a prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software.
- Failure
  - The inability of a system or component to perform its required functions within specified performance requirements.
- Error
  - A difference between a computed result and the correct result.
- Fault
  - A defect in a hardware device or component.
  - An incorrect step, process, or data definition in a computer program.

Hazard analysis의 정의

- Hazard analysis
  - Hazard analysis is the process of identifying and evaluating the hazards of a system, and then either eliminating the hazard or reducing its risk to an acceptable level.
- Safety
  - The term safety is used to mean the extent to which a system is free from system hazard.
- Risk
  - A measure that combines both the likelihood that a system hazard will cause an accident and the severity of that accident.
- Software hazard
  - A software condition that is a prerequisite to an accident.

HAZARD ANALYSIS의 필요성

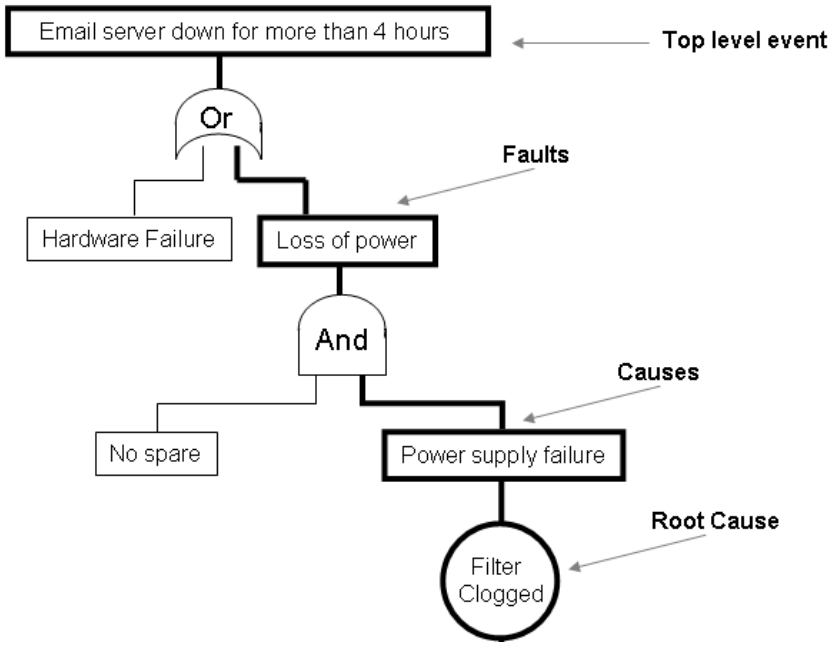
Hazard analysis의 필요성

- System의 accident의 발생으로 인한 피해를 줄이기 위함.
  - Aircraft, Nuclear power plant, Automobile 등 여러 산업 분야에서 hazard analysis를 사용함.

DEVELOPMENT PROCESS와 HAZARD ANALYSIS

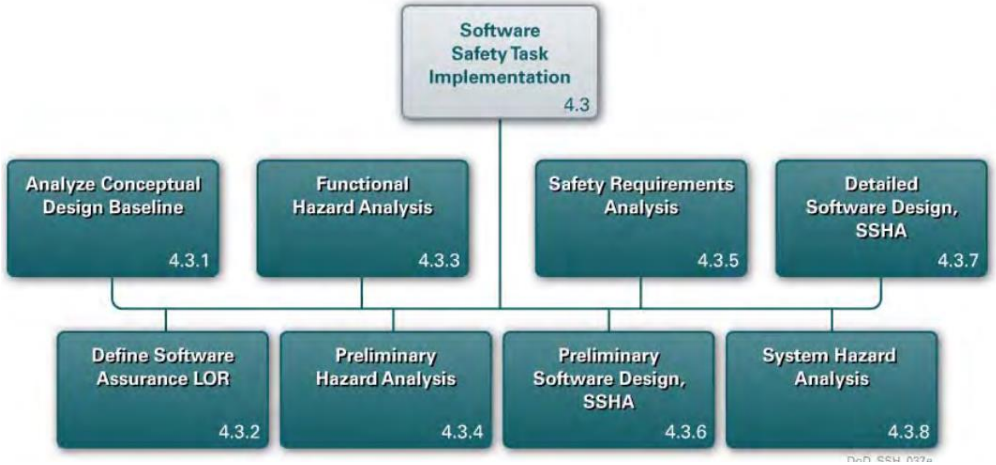
Development process와 hazard analysis

- System 개발의 특정 부분/단계의 분석에 hazard analysis 기법을 적용하여 분석을 수행함.
  - Ex) system의 design specification에 Fault tree analysis를 적용해 system에서 발생할 수 있는 hazard와 원인을 찾아냄



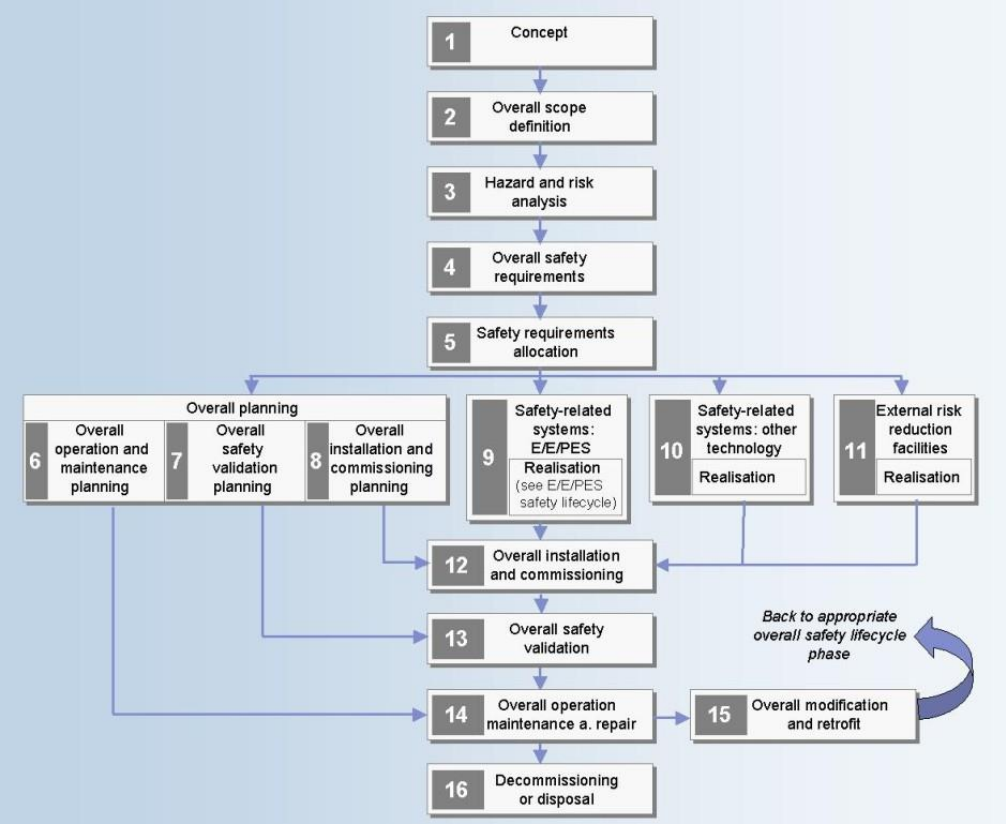
Development process와 hazard analysis

- 각 단계별로 적용해야 하는 기법들을 합쳐 safety life cycle을 만들어서 development process와 병행하여 진행하는 방식을 취하기도 함.
  - Ex) 미국 국방부의 Software system safety engineering process



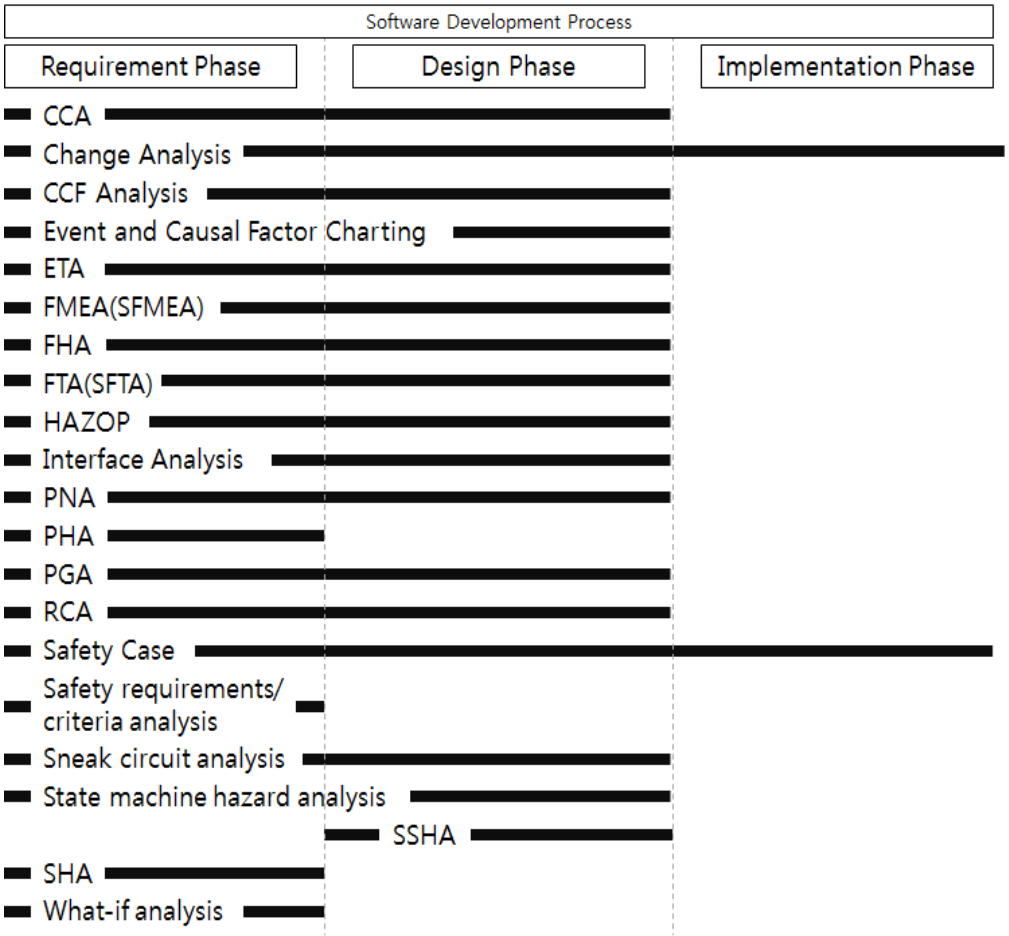
Development process와 hazard analysis

- 각 단계별로 적용해야 하는 기법들을 합쳐 safety life cycle을 만들어서 development process와 병행하여 진행하는 방식을 취하기도 함.
  - Ex) ISO 61508 (*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)*의 safety life cycle



Development process와 hazard analysis

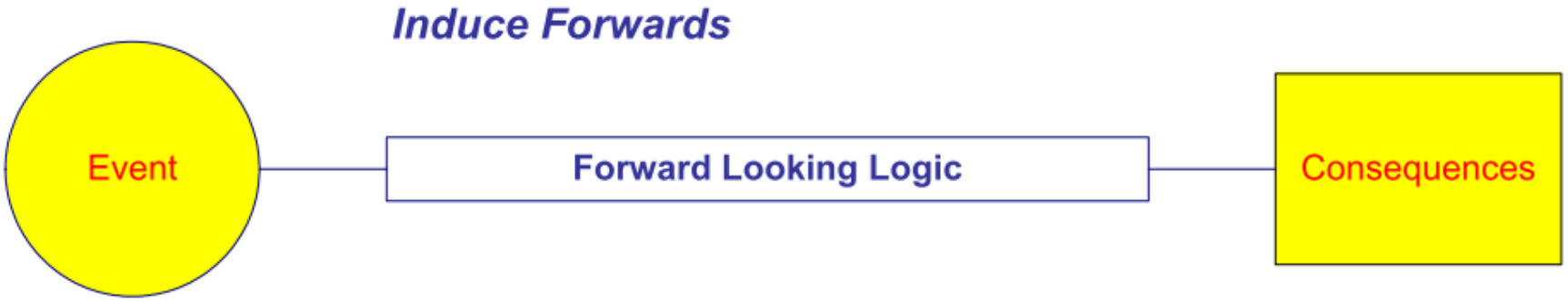
- 소프트웨어 개발 절차에 따라 적용 가능한 hazard analysis 기법



HAZARD ANALYSIS 기법 유형

Hazard analysis 기법 유형

- Inductive modeling
  - 어떤 이벤트의 결과를 유도해 나가는 방식



- Deductive modeling
  - 어떤 이벤트의 원인을 추론해 나가는 방식

Hazard analysis 기법 유형

- Inductive modeling
  - 처음에 피해야 하는 결과가 무엇인지 도출하는 것으로 시작.
  - 이어지는 이벤트는 첫 이벤트에서 가능한 이벤트들로 이루어짐.
  - 단계적인 이벤트들의 조합이 시나리오와 연결됨.
  - 각 시나리오의 결과들을 기술함.

- Deductive modeling
  - 원인을 찾아야 하는 이벤트를 정의하는 것으로 시작.
  - 해당 이벤트를 그 이벤트가 발생하는데 직접적이고 꼭 필요한 원인이 되는 이벤트들로 나눔.
  - 위의 단계를 기본적인 원인(basic cause)이 파악될 때까지 수행함.

Hazard analysis 기법 유형

- Inductive/Forward
  - Accident analysis : risk에 대한 데이터베이스를 기반으로 hazard와 accident의 시나리오를 예측/평가.
  - Change analysis : SW의 요구사항, 디자인 등의 변화로 인해 발생하는 영향력을 추측.
  - Event tree analysis : initial event로부터 potential accident까지 도달하는 과정을 분석하며 단계 별 accident의 발생 확률 계산 가능.
  - Failure mode and effects analysis (FMEA) : subsystem, component, function등 시스템의 하위 단계에서 발생하는 잠재적인 고장 유형이 시스템에 미치는 영향을 분석.

Hazard analysis 기법 유형

- Inductive/Forward
  - Safety requirements/criteria analysis : 디자인 요구사항을 분석하여 위험을 제거하거나 감소시켜 시스템의 위해를 받아들일 수 있는 수준으로 낮춤.
  - Scenario analysis : 물리적/논리적으로 발생할 수 있는 accident의 시나리오를 가정해서 발생할 수 있는 위해 상황을 발견 및 교정함.

Hazard analysis 기법 유형

- Deductive/Backward
  - Common cause failure analysis : 하나의 모듈에서 여러 가지 failure events를 발생시키거나 여러 모듈의 고장을 일으킬 수 있는 공통의 원인을 확인함.
  - Fault tree analysis (FTA) : top event로부터 순차적으로 event의 발생 원인을 탐색함.
  - Preliminary hazard analysis : 간략한 설계 정보를 대상으로 causal source, effect 등을 분석하여 hazard를 완화하기 위한 방법을 제시함.
  - Repetitive failure analysis : 시스템 내의 여러 장비/서브시스템에서 반복적인 실패가 발생할 경우 이를 분석하여 해당 원인을 제거함.
  - Root cause analysis : 시스템의 문제 발생에 대해 문제의 root cause를 찾아서 제거함으로써 문제의 재발을 막음.
  - Sequentially-timed event plot : STEP chart라고 하는 표현 방법을 이용하여 accident가 발생할 때 이벤트들의 sequence를 보고 hazard가 발생할 수 있는 부분을 찾아서 제거함.

Hazard analysis 기법 유형

- Deductive/Backward
  - Sneak circuit analysis : 시스템의 의도치 않은 상황을 발생하게 만드는 실행 path를 찾아서 이 path가 발생하지 않게 시스템의 디자인을 수정함.
  - State machine hazard analysis : 시스템의 모델을 state machine으로 만들어 hazard가 발생할 수 있는 state에 도달할 수 있는지의 여부를 확인하고 이러한 경우가 발생하지 않도록 함.
  - Subsystem hazard analysis : 자세한 시스템 디자인을 대상으로 컴포넌트 레벨에서 발생할 수 있는 hazard의 탐색 및 원인 분석을 수행.
  - System hazard analysis : 시스템 레벨의 hazard에 대한 탐색 및 원인 분석을 수행함. Human error등도 포함됨.
  - Systems theoretic process analysis : system theory 기반의 accident model을 이용하여 컴포넌트간의 상호작용에서 발생할 수 있는 hazard와 그 원인을 확인.

Hazard analysis 기법 유형

- Inductive + deductive
  - Cause consequence analysis : initial event로부터 발생하는 사건들의 sequence의 결과를 확인하고 분석하고 sequence 단계 별 원인 파악 수행.
  - Event and causal factor charting : 사건의 원인이 되는 causal factor와 사건 사이의 인과관계를 차트로 나타내서 사건의 원인 분석 및 미래의 사건에 대한 예측 수행.
  - Hazard and operability analysis (HAZOP) : 설비의 오작동이나 조작의 실수 가능성을 최소화하기 위한 시스템의 deviation을 제시하며, guideword를 이용해 deviation의 원인과 이의 결과들을 검토하고 대책을 수립.

Hazard analysis 기법 유형

- Inductive + deductive
  - Petri net analysis : Petri net diagram을 이용해 시스템의 설계에서 주로 타이밍과 관련하여 발생할 수 있는 hazard를 찾고 이에 대한 원인 분석 및 예측 수행 가능.
  - Probabilistic risk assessment : Event tree와 fault tree를 이용해 hazard를 분석하고 이들의 발생 확률과 심각도를 통해 risk를 계산함.
  - Safety case : 시스템이 만족해야 할 goal을 설정하고 이에 대한 argument와 evidence를 통해 시스템이 만족해야 할 안전성을 확보하도록 함.

HAZARD ANALYSIS 기법들

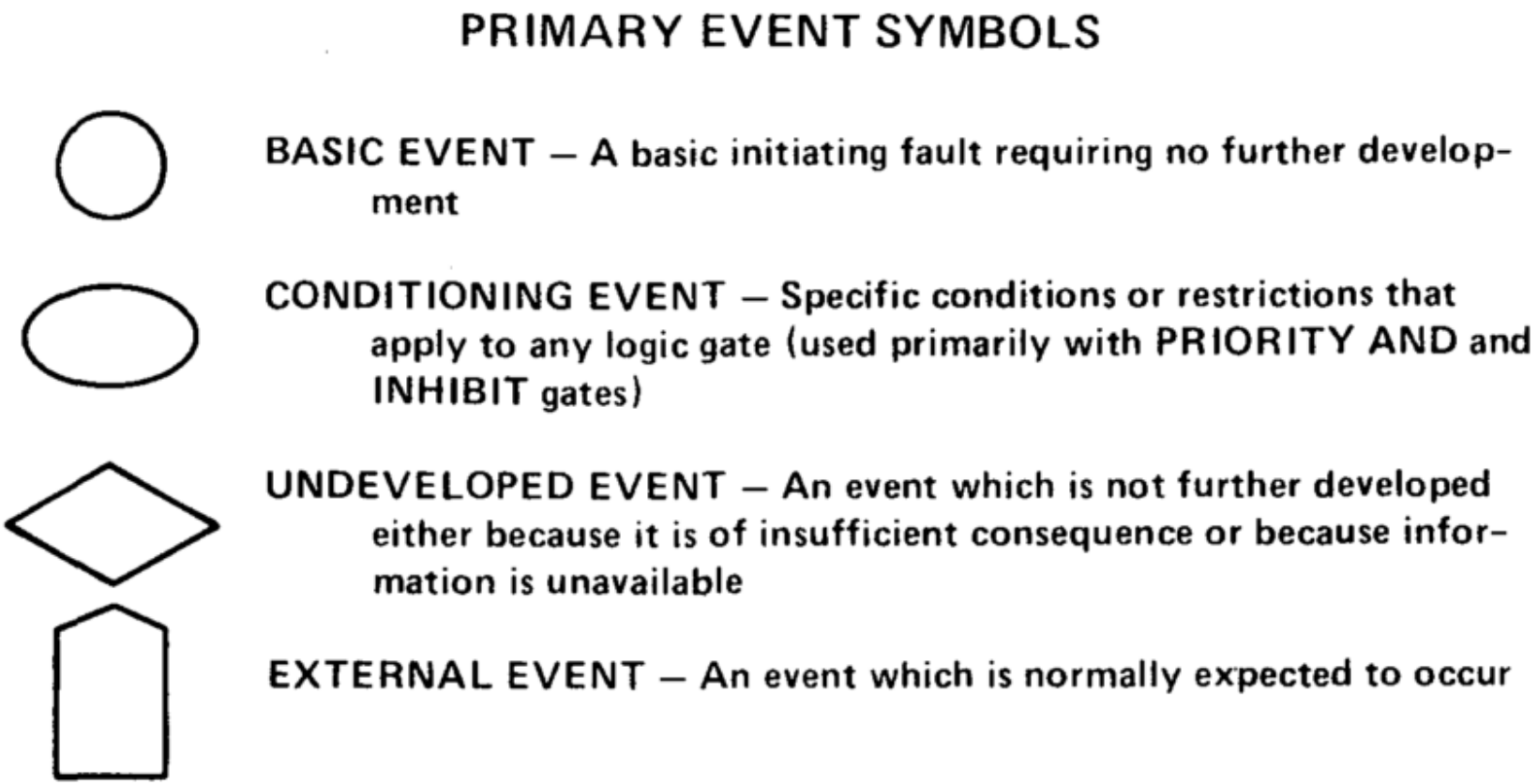
Hazard analysis 기법들 - Fault tree analysis

- 사용 이유
  - Failure의 모든 원인을 찾기 위함.
  - 시스템의 취약점을 찾기 위함.
  - 디자인의 신뢰성과 안전성을 평가하기 위함.
  - Human error가 미치는 영향을 확인하기 위함.
  - Failure에 영향을 주는 요소들의 우선순위를 매기기 위함.
  - Failure의 확률과 영향을 주는 요소들을 양적으로 분석하기 위함.

Hazard analysis 기법들 - Fault tree analysis

- 표기법

Event

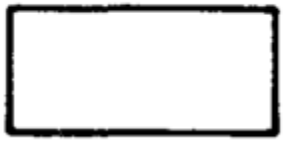


Hazard analysis 기법들 - Fault tree analysis

- 표기법

Event

INTERMEDIATE EVENT SYMBOLS

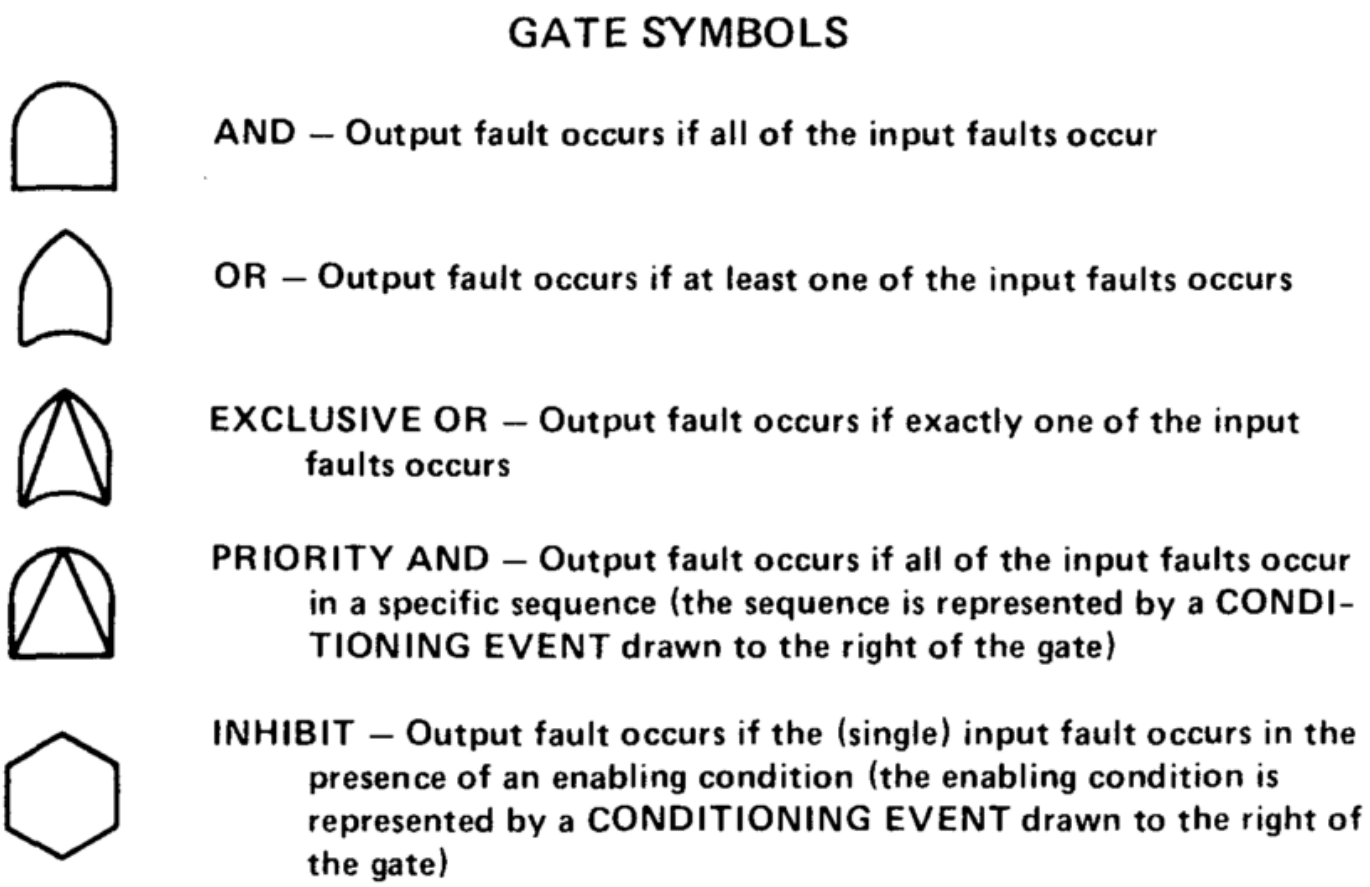


INTERMEDIATE EVENT – A fault event that occurs because of one or more antecedent causes acting through logic gates

Hazard analysis 기법들 - Fault tree analysis

- 표기법

Gate



Hazard analysis 기법들 - Fault tree analysis

- 표기법

Transfer

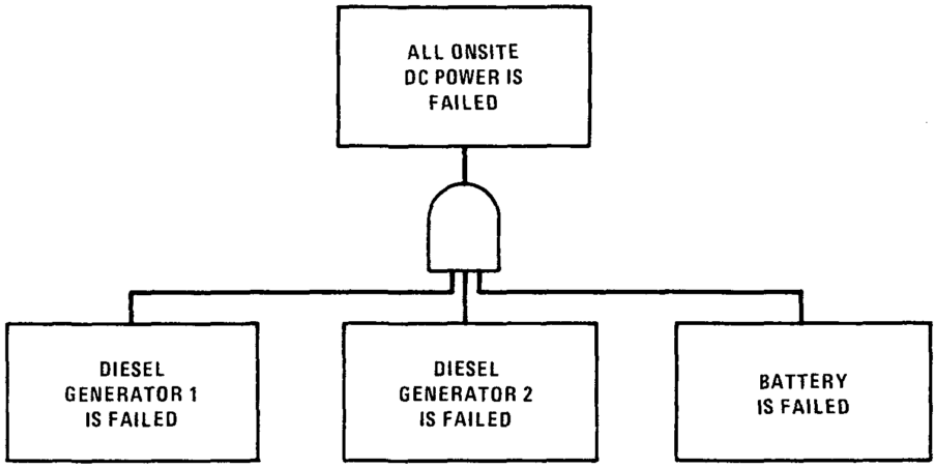
TRANSFER SYMBOLS

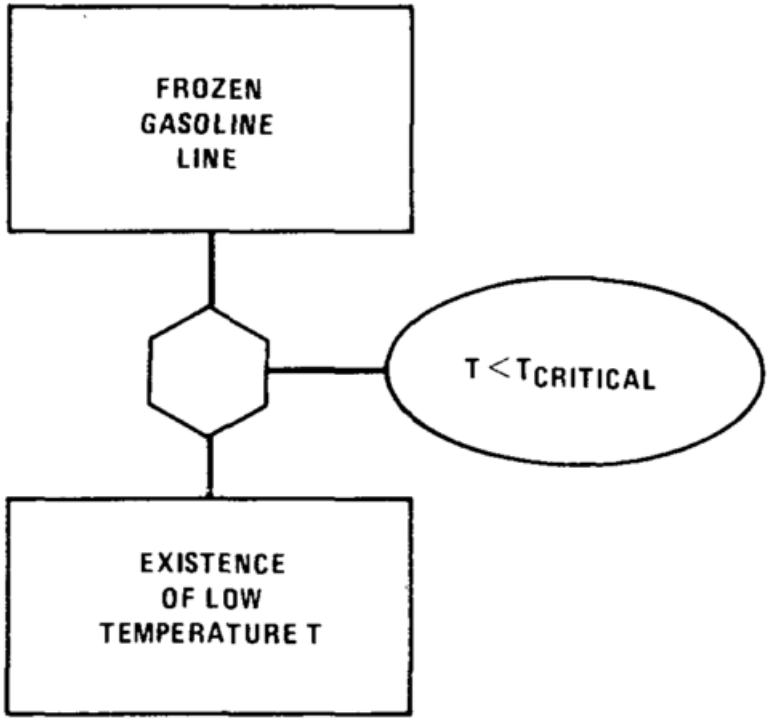
TRANSFER IN – Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)

TRANSFER OUT – Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

Hazard analysis 기법들 - Fault tree analysis

- 작성 단계





Hazard analysis 기법들 - Fault tree analysis

- 장점
  - Top event가 발생할 수 있는 여러 요소들을 명시적으로 보여줌.
  - Fault tree를 작성하는 과정에서 해당 기능에 대한 logic과 basic cause들에 대한 이해를 높일 수 있음.
  - Top event를 양적 질적으로 판단할 수 있는 시스템적인 프레임워크를 제공함.

Hazard analysis 기법들 - Fault tree analysis

- 적용 사례
  - 이란의 시멘트공장에서 plant의 문제 분석에 적용

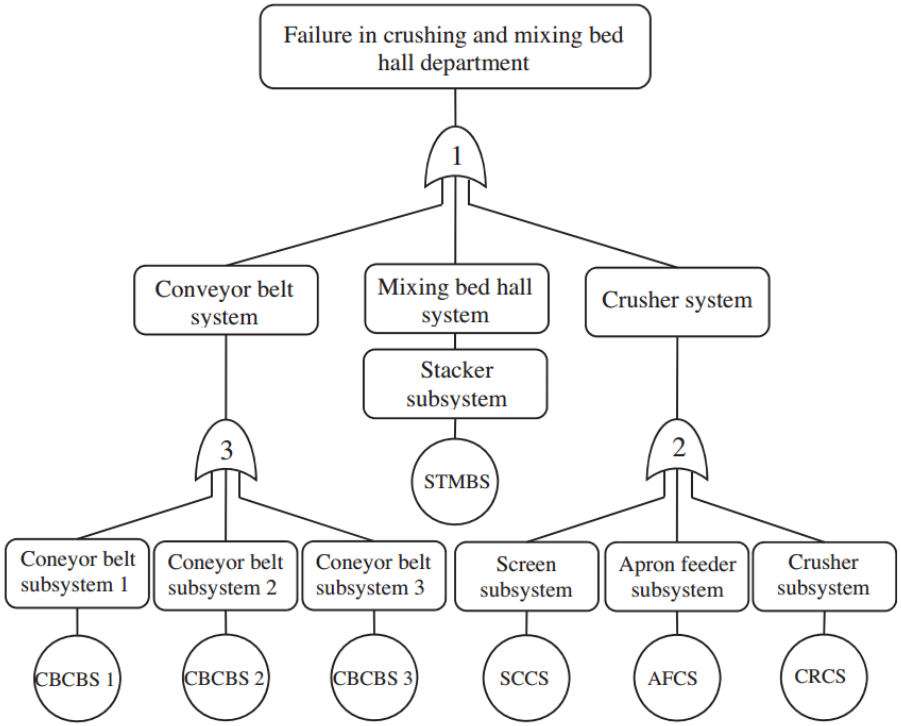


Fig. 2. Fault tree of crushing and mixing bed hall department.

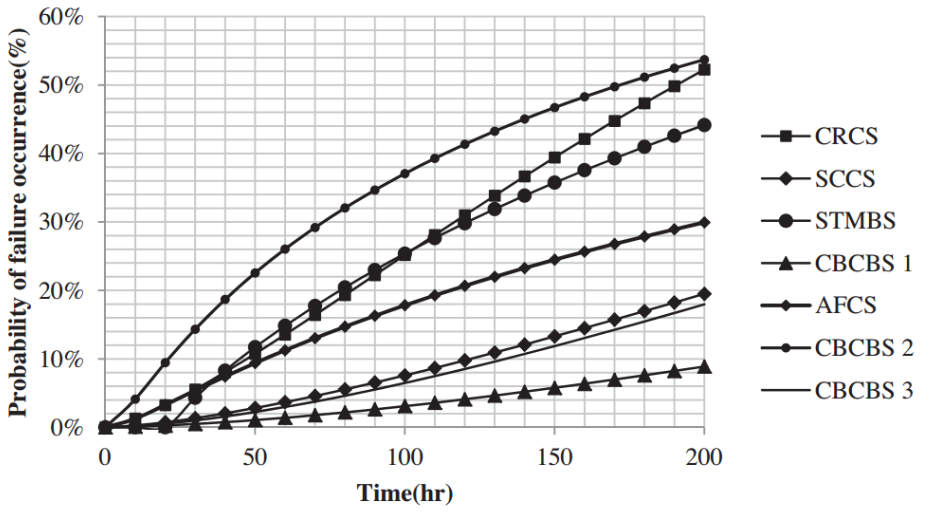
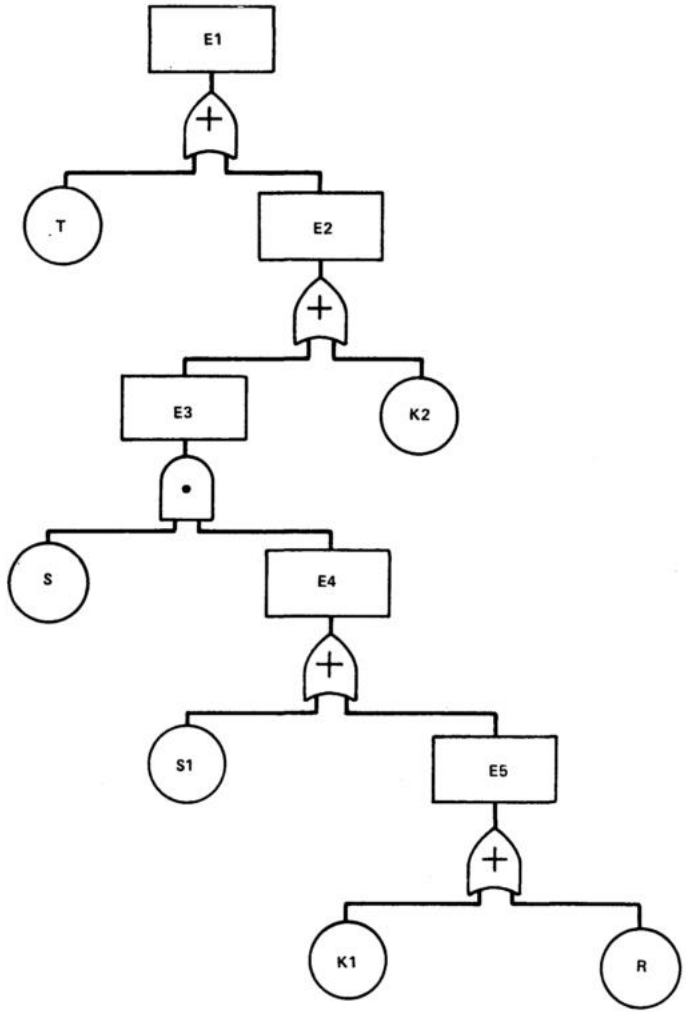


Fig. 4. Probability of failure occurrence for basic events.

Hazard analysis 기법들 - Fault tree analysis

- 추가사항
  - Cut set
    - A list of failure events such that if they occur then so does the top event.
  - Minimal cutset
    - A list of minimal, necessary and sufficient conditions for the occurrence of the top event.
  - 오른쪽의 fault tree에서 아래의 노드 조합이 minimal cut set에 해당함.

T
K2
S · K1
S · R
S · S1

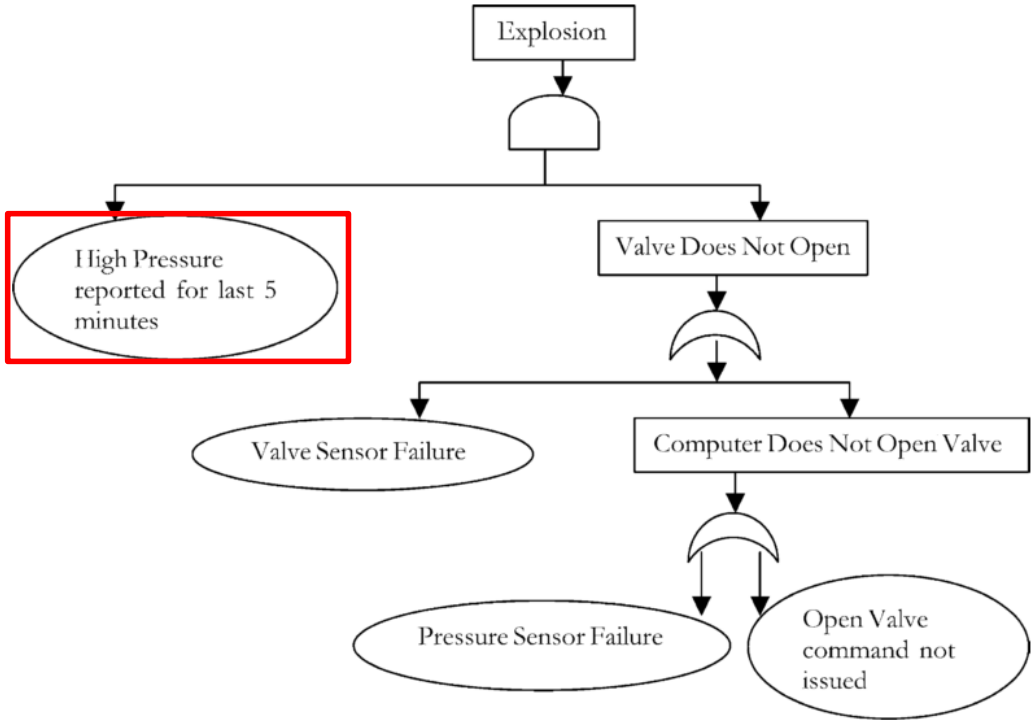


Hazard analysis 기법들 - Fault tree analysis

- 추가사항
  - Software fault tree analysis
    - 시스템의 hazard 발생에 영향을 주는 software를 찾기 위한 기법.
    - 소프트웨어의 failure로 인해 발생하는 undesired event를 최상위 노드로 두고 이 이벤트의 발생 원인이 되는 소프트웨어의 동작을 찾음.

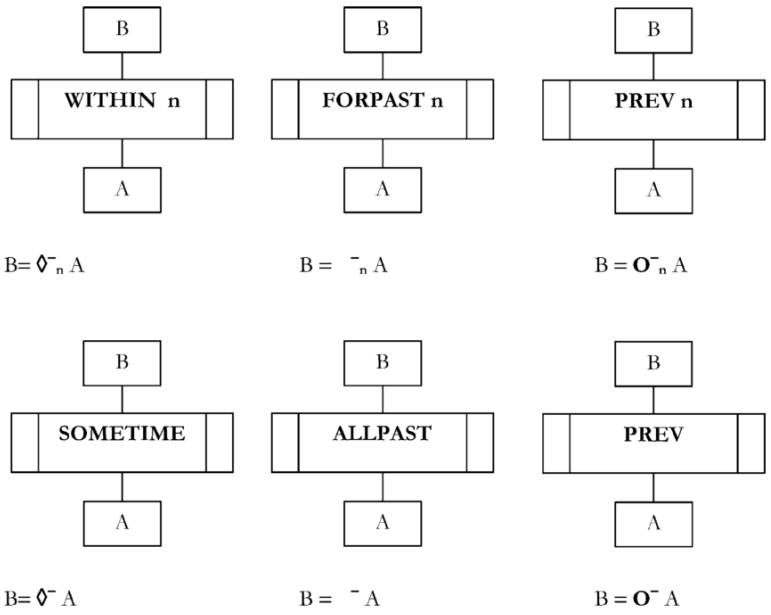
Hazard analysis 기법들 - Fault tree analysis

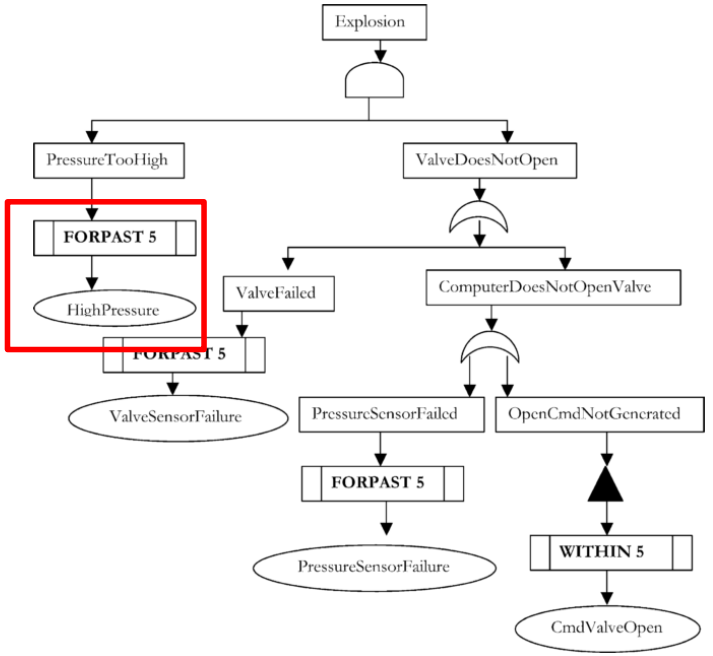
- 추가사항
  - Temporal fault tree
    - Fault tree에서 지원하는 표기법만으로는 시간과 관련된 내용을 나타내기가 어려움.
    - 시간과 관련된 사항을 나타내기 위한 temporal gate를 추가하여 fault tree를 생성.



Hazard analysis 기법들 - Fault tree analysis

- 추가사항
  - Temporal fault tree
    - Fault tree에서 지원하는 표기법만으로는 시간과 관련된 내용을 나타내기가 어려움.
    - 시간과 관련된 사항을 나타내기 위한 temporal gate를 추가하여 fault tree를 생성.



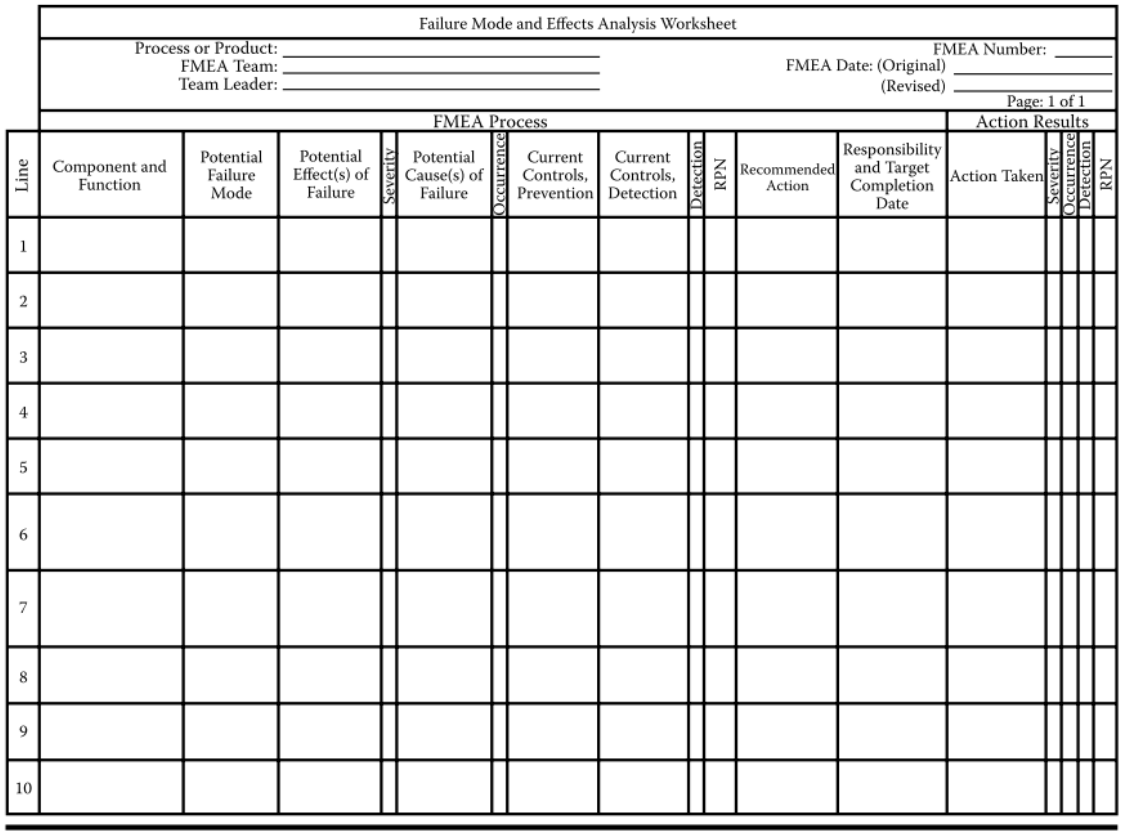


Hazard analysis 기법들 - FMEA

- 사용 이유
  - Failure mode and effects analysis
  - 제품 및 공정에서 발생할 수 있는 잠재적인 고장 유형과 그 영향을 인식.
  - 고장의 원인 및 발생 과정을 파악.
  - 고장의 검출/관리방법을 평가.
  - 위의 과정을 통한 고장 유형의 우선순위 파악 및 이에 대한 대책을 세움으로써 고장의 위험을 사전에 예방.

Hazard analysis 기법들 - FMEA

- 작성 단계
  - 적용 분야 별 FMEA를 위한 worksheet가 있어서 분석 프로세스를 따라 worksheet를 채워나감.



Failure Mode and Effects Analysis Worksheet

Process or Product: _____ FMEA Number: _____
FMEA Team: _____ FMEA Date: (Original) _____
Team Leader: _____ (Revised) _____

Page: 1 of 1

	FMEA Process											Action Results				
Line	Component and Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) of Failure	Occurrence	Current Controls, Prevention	Current Controls, Detection	Detection	RPN	Recommended Action	Responsibility and Target Completion Date	Action Taken	Severity	Occurrence	Detection	RPN
1																	
2																	
3																	
4																	
5																	
6																	
7																	
8																	
9																	
10																	

Hazard analysis 기법들 - FMEA

- 작성 단계
  1. Review the process or product.
  2. Brainstorm potential failure mode.
  3. List potential effects of each failure mode.
  4. Assign a severity ranking for each effect.
  5. Assign an occurrence ranking for each failure mode.
  6. Assign a detection ranking for each failure mode and/or effect.
  7. Calculate the risk priority number for each effect.
  8. Prioritize the failure modes for action.
  9. Take action to eliminate or reduce the high-risk failure modes.
  10. Calculate the resulting RPN as the failure modes are reduced or eliminated.

Hazard analysis 기법들 - FMEA

- 작성 단계
  - 위험우선순위 (RPM, Risk Priority Number)
  - 심각도 (Severity) * 발생도 (Occurrence) * 검출도 (Detection)

Table 8.2a (Generic) Design FMEA Severity Evaluation Criteria

Effect	Criteria: Severity of Effect on Product (Customer Effect)	Rank
Failure to Meet Safety and/or Regulatory Requirements	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulations without warning.	10
	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulations with warning.	9
Loss or Degradation of Primary Function	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation).	8
	Degradation of primary function (vehicle operable, but at reduced level of performance).	7
Loss or Degradation of Secondary Function	Loss of primary function (vehicle inoperable, but comfort/convenience functions inoperable).	6
	Degradation of primary function (vehicle inoperable, but comfort/convenience functions at reduced level of performance).	5
Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by most customers (>75%).	4
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by many customers (50%).	3
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by discriminating customers (<25%).	2
No effect	No discernible effect.	1

Source: Reprinted from Potential Failure Mode and Effects Analysis, (FMEA 4th edition, 2008 Manual) with permission of DaimlerChrysler, Ford and GM Supplier Quality Requirements Task Force.

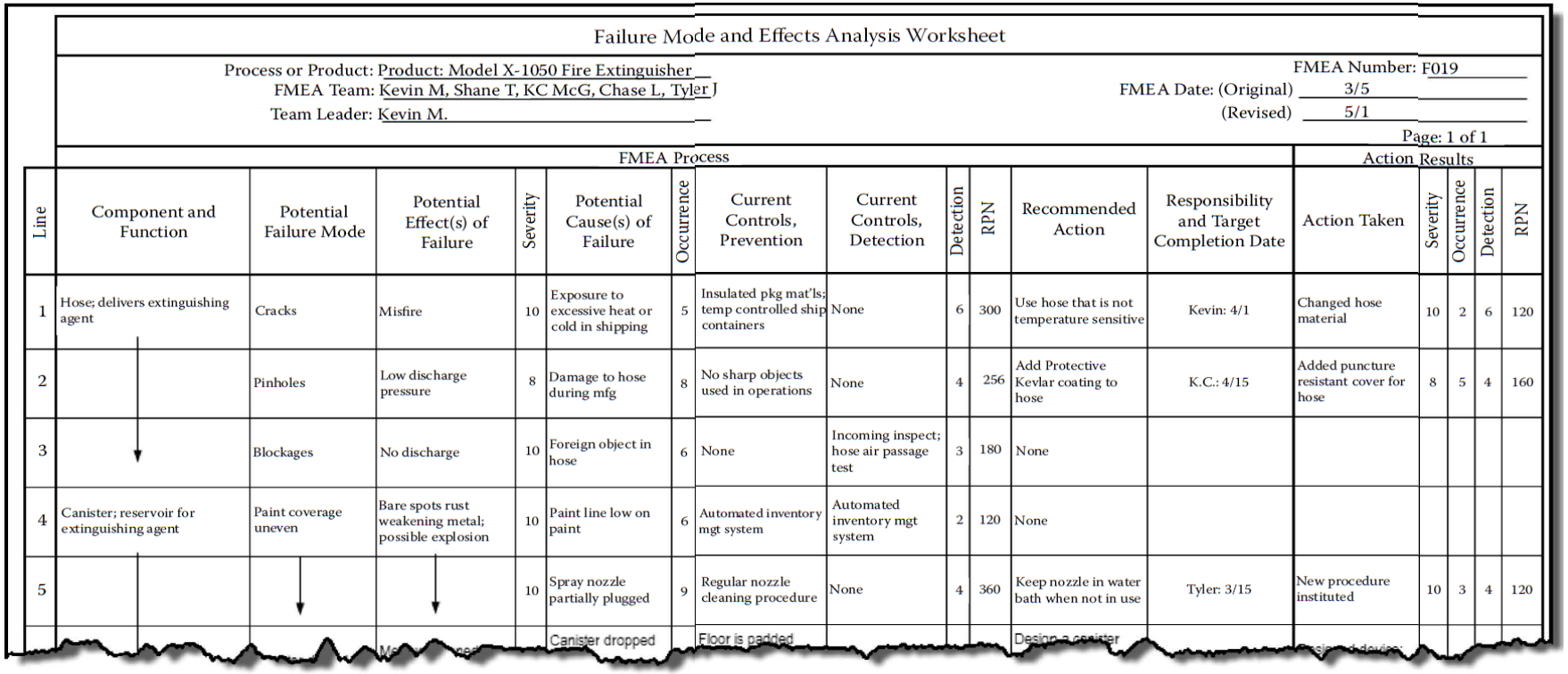
Table 8.2b (Generic) Process FMEA Severity Evaluation Criteria

Effect	Criteria: Severity of Effect on Product (Customer Effect)	Rank	Effect	Criteria: Severity of Effect on Process (Manufacturing/Assembly Effect
Failure to Meet Safety and/or Regulatory Requirements	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulations without warning.	10	Failure to Meet Safety and/or Regulatory Requirements	May endanger operator (machine or assembly) without warning.
	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulations with warning.	9		May endanger operator (machine or assembly) with warning.
Loss or Degradation of Primary Function	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation).	8	Major Disruption	100% of product may have to be scrapped. Line shutdown or stop ship.
	Degradation of primary function (vehicle operable, but at reduced level of performance).	7	Significant Disruption	A portion of the production run may have to be scrapped. Deviation from primary process including decreased line speed or added manpower.
Loss or Degradation of Secondary Function	Loss of secondary function (vehicle inoperable but comfort/convenience functions inoperable).	6	Moderate Disruption	100% of production run may have to be reworked off line and accepted.
	Degradation of secondary function (vehicle inoperable but comfort/convenience functions at a reduced level of performance).	5		A portion of the production run may have to be reworked off line and accepted.
Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by most customers (>75%).	4	Moderate Disruption	100% of production run may have to be reworked in-station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by many customers (50%).	3		A portion of the production run may have to be reworked in-station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by discriminating customers (<25%).	2	Minor Disruption	Slight inconvenience to process, operation, or operator
No effect	No discemible effect.	1	No effect	No discemible effect.

Source: Reprinted from Potential Failure Mode and Effects Analysis, (FMEA 4th edition, 2008 Manual) with permission of DaimlerChrysler, Ford and GM Supplier Quality Requirements Task Force.

Hazard analysis 기법들 - FMEA

- 작성 단계



Failure Mode and Effects Analysis Worksheet

Process or Product: Product: Model X-1050 Fire Extinguisher
FMEA Team: Kevin M, Shane T, KC McG, Chase L, Tyler J
Team Leader: Kevin M.

FMEA Number: F019
FMEA Date: (Original) 3/5
(Revised) 5/1

Page: 1 of 1

	FMEA Process											Action Results				
Line	Component and Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) of Failure	Occurrence	Current Controls, Prevention	Current Controls, Detection	Detection	RPN	Recommended Action	Responsibility and Target Completion Date	Action Taken	Severity	Occurrence	Detection	RPN
1	Hose; delivers extinguishing agent	Cracks	Misfire	10	Exposure to excessive heat or cold in shipping	5	Insulated pkg mat'ls; temp controlled ship containers	None	6	300	Use hose that is not temperature sensitive	Kevin: 4/1	Changed hose material	10	2	6	120
2		Pinholes	Low discharge pressure	8	Damage to hose during mfg	8	No sharp objects used in operations	None	4	256	Add Protective Kevlar coating to hose	K.C.: 4/15	Added puncture resistant cover for hose	8	5	4	160
3		Blockages	No discharge	10	Foreign object in hose	6	None	Incoming inspect; hose air passage test	3	180	None						
4	Canister; reservoir for extinguishing agent	Paint coverage uneven	Bare spots rust weakening metal; possible explosion	10	Paint line low on paint	6	Automated inventory mgt system	Automated inventory mgt system	2	120	None						
5				10	Spray nozzle partially plugged	9	Regular nozzle cleaning procedure	None	4	360	Keep nozzle in water bath when not in use	Tyler: 3/15	New procedure instituted	10	3	4	120
					Canister dropped		Floor is padded				Design a canister						

Hazard analysis 기법들 - FMEA

- 장점
  - 체계적으로 고장 유형으로부터 인과관계를 규명함으로써 고장 유형에 대한 파악 및 확인이 쉬움.
  - 기법 자체의 이해 및 적용이 쉬움.

- 단점
  - 구성 요소간의 상세한 연관관계나 종속성에 대한 정보가 없으므로 분석을 수행하기 위해 해당 분야의 전문가가 필요함.
  - 고장 유형과 관련되지 않은 위해도 분석에 대한 내용이 부족함.

Hazard analysis 기법들 - FMEA

- 적용 사례
  - SW를 대상으로 FMEA를 수행하여 safety-related application software를 분석.
  - 전체 시스템을 대상으로 hazard analysis를 수행하고, SW FMEA를 각각의 프로그램에 적용.

Software FMEA analysis results for "Channel 3 Equipment Check" sub-module.

Sub-module	Failure mode	Failure cause	Failure effect	Failure detection/comments
Other Channel 3 Equipment Check	Omission	Omission in equipment diagnosis or heartbeat monitoring functions	Periodic automatic test is affected adversely	There is no update procedure for a variable AL_1_ATIP_ATIPD_PHBC.→ Channel A, B, and C cannot recognize when the channel D HB is malfunctioning
	Incorrect realization	There is an error in equipment diagnosis or heartbeat monitoring functions	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Unintended addition	Additional functions in equipment diagnosis or heartbeat monitoring functions	There is no effect on equipment diagnosis	No failure detected
	Function interaction	Inappropriate location of implementation of a function	There is an degradation in this module	No failure detected
	Input definition	Wrong input definition, assignment, address, or type definition	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Input value	Wrong min/max limits or initialization value in heartbeat coefficients	Malfunction in monitoring of channel D ATIP heartbeat signal	No failure detected
	Input timing	An input variable is used before updating	Delay in processing the input signal	No failure detected
	Input format	Omission/addition of an interver, wrong input number, or input disorder	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Output definition	Wrong output definition, assignment, address, or type definition	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Output value	Wrong assignment of an output value	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Output timing	Wrong timing for generating an output value	Malfunction in Channel 3 equipment diagnosis	No failure detected. (Output from this submodule is correctly used in the next step.)
	Output format	Omission/addition of an interver, wrong output number, or input disorder	Malfunction in Channel 3 equipment diagnosis	No failure detected

Hazard analysis 기법들 - FMEA

- 추가 사항
  - Software FMEA
    - 소프트웨어의 function을 대상으로 FMEA를 수행함.

Element Failure Modes	Fails to execute
	Executes incompletely
	Output incorrect
	Incorrect timing – too early, too late, slow, etc
System Failure Modes	Input value incorrect (logically complete set)
	Output value corrupted (logically complete set)
	Blocked interrupt
	Incorrect interrupt return (priority, failure to return)
	Priority errors
	Resource conflict (logically complete set)

Hazard analysis 기법들 - HiP-HOPS

- 사용 이유
  - 현대의 전자 시스템의 복잡도는 증가하고 있으며 이에 따라 기존의 hazard analysis 기법을 적용하는데 문제가 생김.
  - 시스템에 대한 여러 safety 기법들의 적용 시 일관성의 부족.
    - 분석 과정에서 일관성의 부족에서 생기는 문제들을 처리.
    - Lifecycle동안 일관된 표기법을 이용해 분석을 수행함으로써 분석 결과의 일관성을 보장할 필요가 있음.
  - Safety analysis의 결과들을 다시 high-level의 functional failure analysis (FFA) 결과와 연관 짓기 어려움.
    - Low-level component의 failure가 hazardous system malfunction에 미치는 영향에 대한 분석이 어려움.
  - 계층적으로 표현된 복잡한 시스템의 통합적인 평가를 가능하게 함.

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  1. 시스템 레벨
     1. 시스템 디자인을 functional block diagram으로 나타냄.
     2. Functional block diagram에서 발생할 수 있는 문제들을 찾기 위해 FFA를 수행함.
     3. FFA에서 찾아낸 single functional failure들간의 조합으로 발생할 수 있는 문제들을 분석함.
  2. 컴포넌트 레벨
     1. 시스템 디자인으로부터 hierarchical model을 작성함.
     2. Hierarchical model을 대상으로 IF-FMEA를 수행함.
     3. IF-FMEA를 이용해 모든 컴포넌트의 failure behavior를 찾음.
  3. 통합
     1. FFA의 분석 결과와 IF-FMEA의 분석 결과를 연결하기 위해 fault tree의 자동 생성을 사용함.

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계

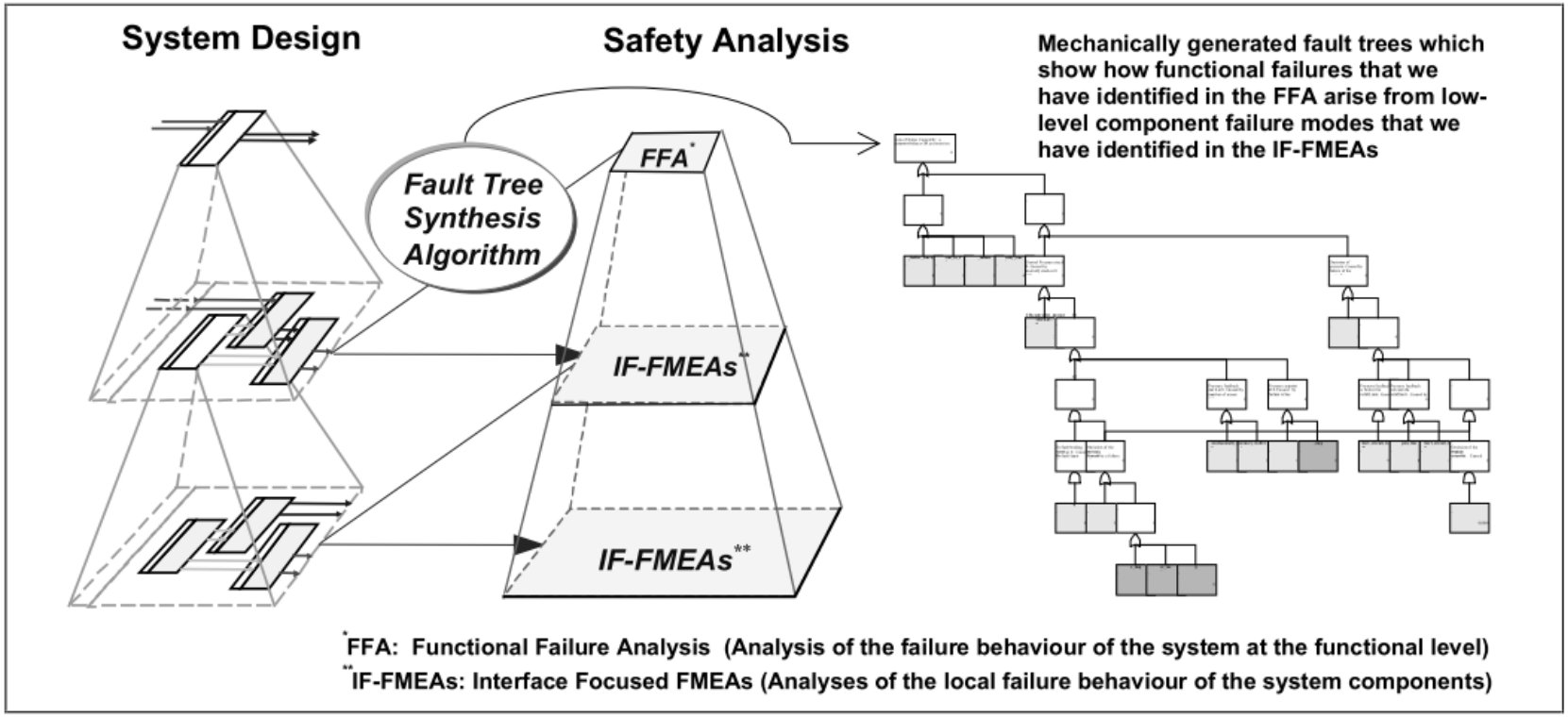


Fig. 1. Overview of Design and Safety Analysis in HiP-HOPS

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  - Functional failure analysis (FFA)
    - 일반적인 FMEA와 마찬가지로 테이블을 작성함.
    - Internal malfunction으로 발생하는 component failure를 설명하기 위해 사용.
    - 컴포넌트들의 입력과 출력의 상호작용에서 발생하는 failure의 발견, 완화 및 전파를 분석하는 데 사용함.

Failure	ID	Effects on System	Severity	Detection	Recovery	Recommendation
OYB: Loss of Braking (omission) when there is braking intention	FL3	The car tends to drift to the side -30% stability -18/-32% braking -15% steerability In the worst case the drift is opposite to the drivers intention	Critical	Locally, using feedback from pressure sensor Remotely, by the status reporter and monitor tasks	Not Possible	In addition, the failure can be detected by a global rotational acceleration sensor. An Electronic Stability Program device may handle the problem (this is out of the scope of this BBW system)
CNB: Unintended Braking (Commission) when there is no braking intention	FL4	The car tends to drift to the side	Critical	It is possible in certain cases by comparing the state of the pedal with the pressure sensor feedback from the wheel	Release actuator	Detection algorithm should be sufficient to detect pedal sensor failures and internal corruption of the pedal messages. There should be provisions to keep commission failures temporally limited

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  - Interface focused FMEA (IF-FMEA)
    - 일반적인 FMEA와 마찬가지로 테이블을 작성함.
    - Internal malfunction으로 발생하는 component failure를 설명하기 위해 사용.
    - 컴포넌트들의 입력과 출력의 상호작용에서 발생하는 failure의 발견, 완화 및 전파를 분석하는 데 사용함.

Table 1. Excerpt of IF-FMEA of PEDAL task

Output Failure Mode	Description of output failure	Input Deviation Logic	Component Malfunction Logic	λ (f/h)
O-PEDAL1. Driver_msg	Omission of PEDAL1 output (braking demand). It can be caused by task malfunction or out of range failures of both pedal sensors	(V>max-PS1.value | V<min-PS1.value) & (V>max-PS2.value | V<min-PS2.value)	PEDAL1.task_ malfunction	1.00E-07
Vs_0-PEDAL1. Driver_msg	PEDAL1 output (braking demand) stuck at 0. It can be caused by memory stuck at 0 failures, or by stuck at minimum failures of both pedal sensors.	Vs_min-PS1.value & Vs_min-PS2.value	PEDAL1.memory_ stuck_at_0	2.00E-07

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  - IF-FMEA expression
    - Fault tree의 자동 생성을 위해 IF-FMEA의 output failure의 원인을 formal grammar로 나타내야 함.
    - 이를 위한 formal grammar의 형태를 정의함.

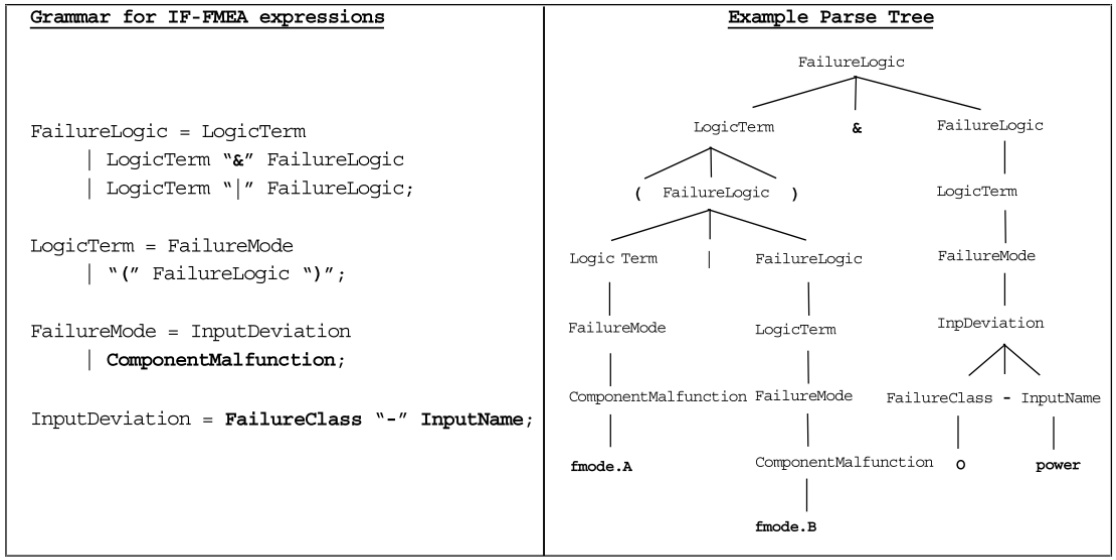


Fig. 2. Formal grammar for IF-FMEA expressions and example parse tree

"(fmode.A|fmode.B)&O-power"

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  1. 시스템 레벨
     1. 시스템 디자인을 functional block diagram으로 나타냄.

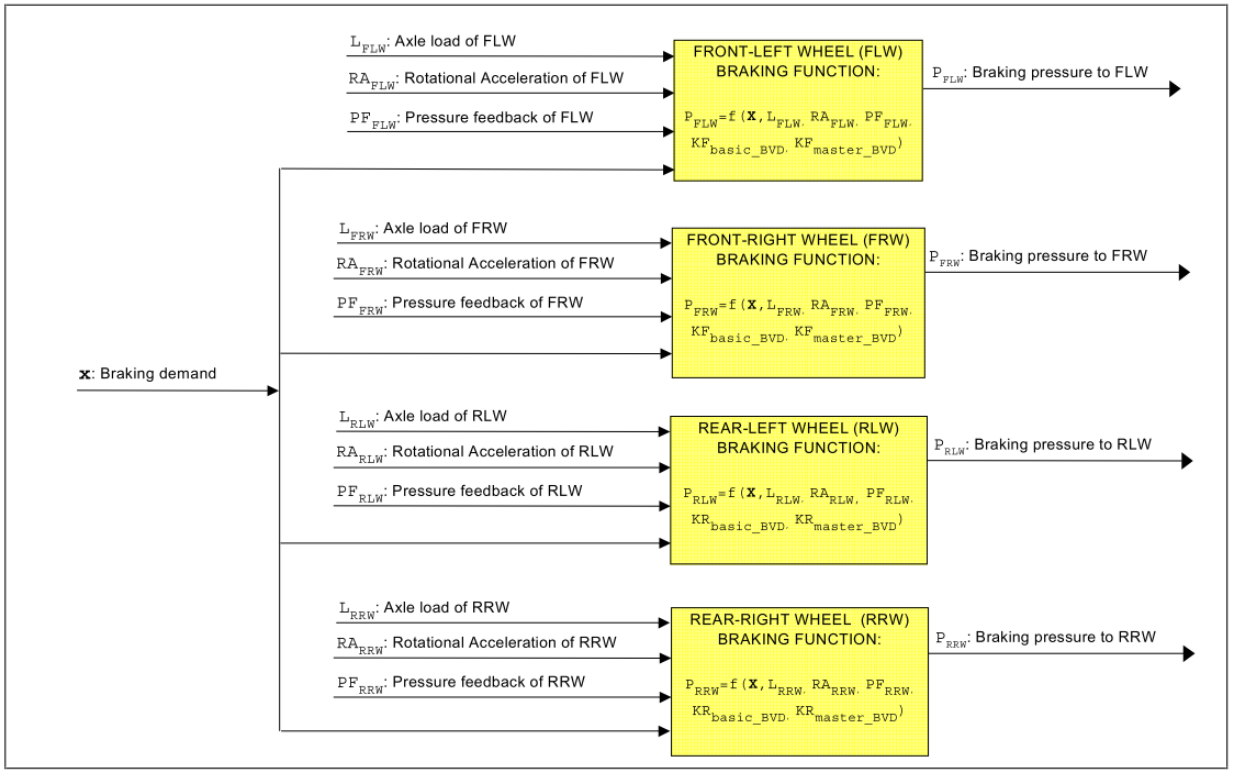


Fig. 4. Abstract Functional Model of the Brake by Wire System

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  1. 시스템 레벨
     2. Functional block diagram에서 발생할 수 있는 문제들을 찾기 위해 FFA를 수행함.
     3. FFA에서 찾아낸 single functional failure들간의 조합으로 발생할 수 있는 문제들을 분석함.

Failure	ID	Effects on System	Severity	Detection	Recovery	Recommendation
OYB: Loss of Braking (omission) when there is braking intention	FL3	The car tends to drift to the side -30% stability -18/-32% braking -15% steerability In the worst case the drift is opposite to the drivers intention	Critical	Locally, using feedback from pressure sensor Remotely, by the status reporter and monitor tasks	Not Possible	In addition, the failure can be detected by a global rotational acceleration sensor. An Electronic Stability Program device may handle the problem (this is out of the scope of this BBW system)
CNB: Unintended Braking (Commission) when there is no braking intention	FL4	The car tends to drift to the side	Critical	It is possible in certain cases by comparing the state of the pedal with the pressure sensor feedback from the wheel	Release actuator	Detection algorithm should be sufficient to detect pedal sensor failures and internal corruption of the pedal messages. There should be provisions to keep commission failures temporally limited

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  2. 컴포넌트 레벨
     1. 시스템 디자인으로부터 hierarchical model을 작성함.

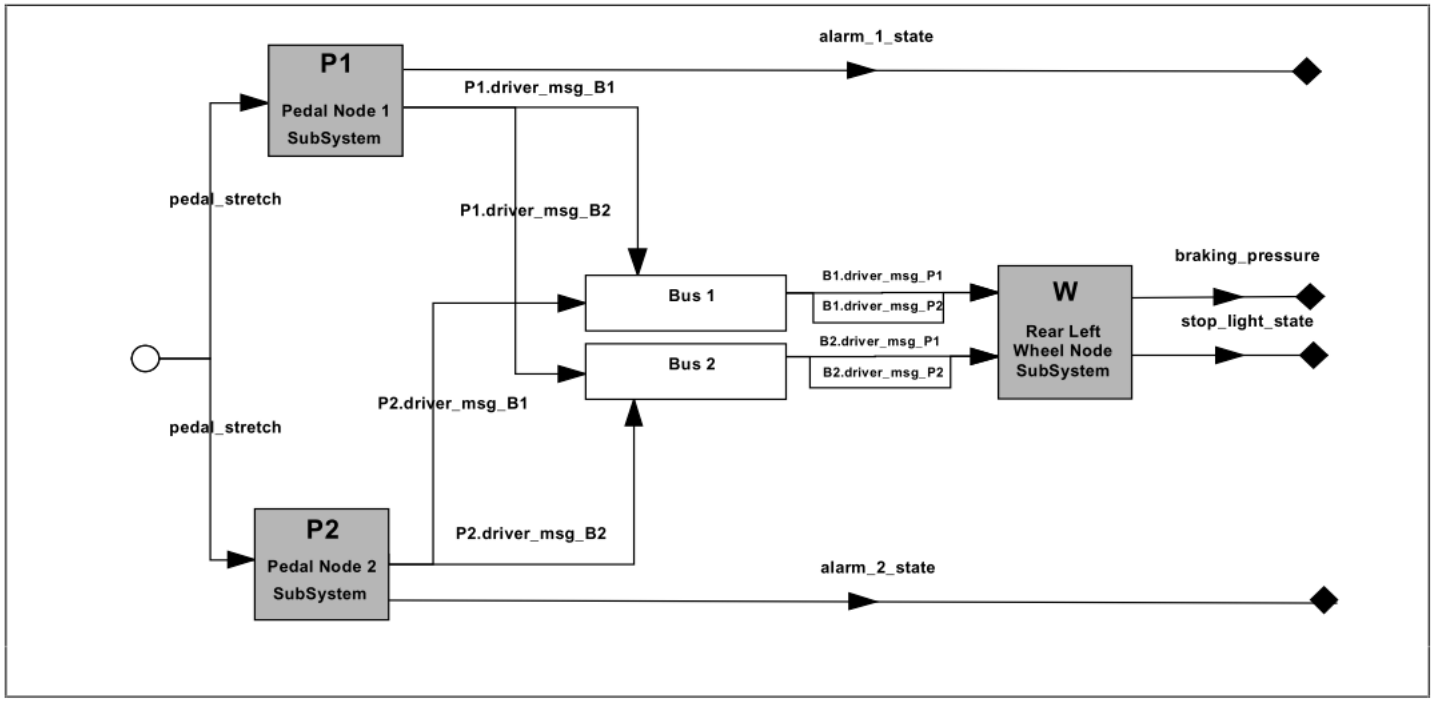


Fig. 5. Top level of the hierarchical model of the BBW system

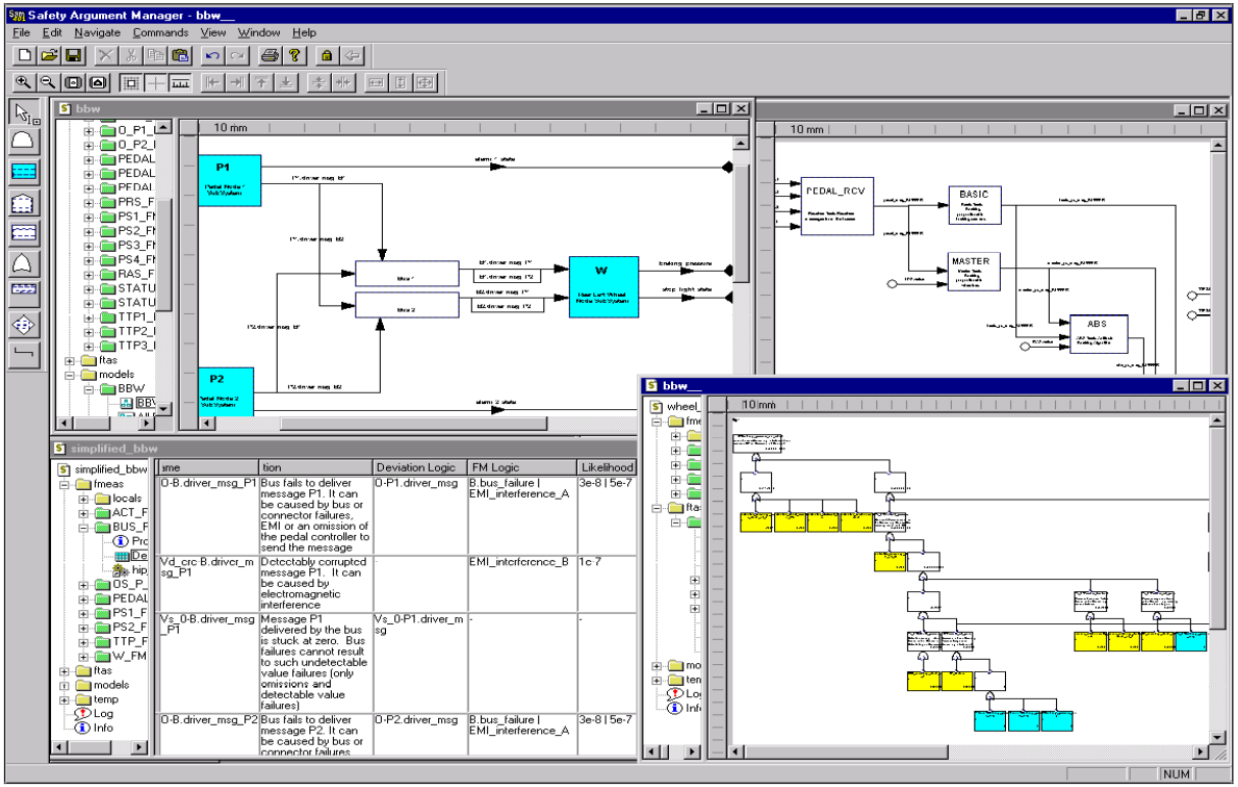
Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  2. 컴포넌트 레벨
     2. Hierarchical model을 대상으로 IF-FMEA를 수행함.
     3. IF-FMEA를 이용해 모든 컴포넌트의 failure behavior를 찾음.

Output Failure Mode	Description of output failure	Input Deviation Logic	Component Malfunction Logic	λ (f/h)
O-PEDAL1. Driver_msg	Omission of PEDAL1 output (braking demand). It can be caused by task malfunction or out of range failures of both pedal sensors	(V>max-PS1.value | V<min-PS1.value) & (V>max-PS2.value | V<min-PS2.value)	PEDAL1.task_ malfunction	1.00E-07
Vs_0- PEDAL1. Driver_msg	PEDAL1 output (braking demand) stuck at 0. It can be caused by memory stuck at 0 failures, or by stuck at minimum failures of both pedal sensors.	Vs_min-PS1.value & Vs_min-PS2.value	PEDAL1.memory_ stuck_at_0	2.00E-07

Hazard analysis 기법들 - HiP-HOPS

- 작성 단계
  3. 통합
     1. FFA의 분석 결과와 IF-FMEA의 분석 결과를 연결하기 위해 fault tree의 자동 생성을 사용함.



Hazard analysis 기법들 - HiP-HOPS

- 장점
  - 일관된 분석 과정 및 결과 제공.
  - High-level의 분석 결과와 low-level의 분석 결과간의 연관성을 잘 보여줄 수 있음.

- 단점
  - Human operator의 상호작용이 적은 전자 시스템의 분석에만 적합함.

Hazard analysis 기법들 - STPA

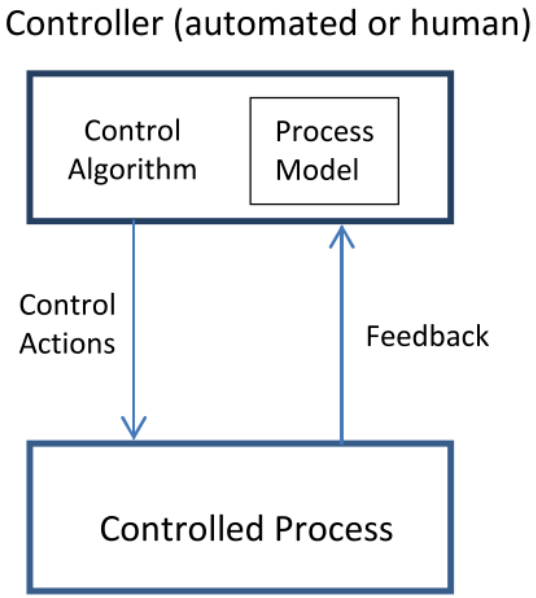
- 사용 이유
  - 디자인의 문제나 안전하지 않은 상호작용에서 발생하는 컴포넌트간 상호작용에서 발생하는 accident를 분석하기 위함.
  - 기술적인 요소만이 아닌 사회적/조직적/관리적 등의 비기술적인 요인들도 안전 요소로 고려하기 위함.

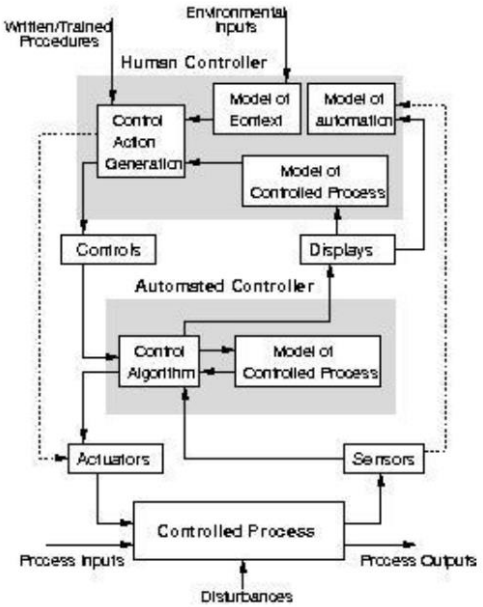
Hazard analysis 기법들 - STPA

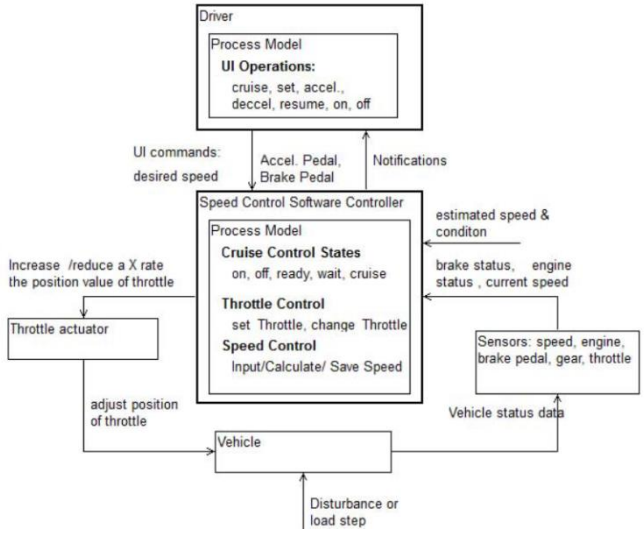
- 작성 단계
  1. 시스템 레벨의 accident와 hazard, safety constraint의 식별
  2. Control structure의 구축
  3. STPA step 1 : Unsafe control action의 식별
  4. STPA step 2 : Unsafe control action의 잠재 원인 식별

Hazard analysis 기법들 - STPA

- 작성 단계
  - Control loop
    - 모든 단계의 control structure에서 나타날 수 있으며, controller가 하위의 controller 또는 controlled process에 control action을 보내고 이에 대한 feedback을 받는 구조로 되어있음.
    - Controller는 controller의 내부 정보/외부 입력 등의 정보들을 나타내는 Process model을 가지며 Process model의 상태와 Control algorithm에 따라 적절한 control action을 내보내게 되어있음.

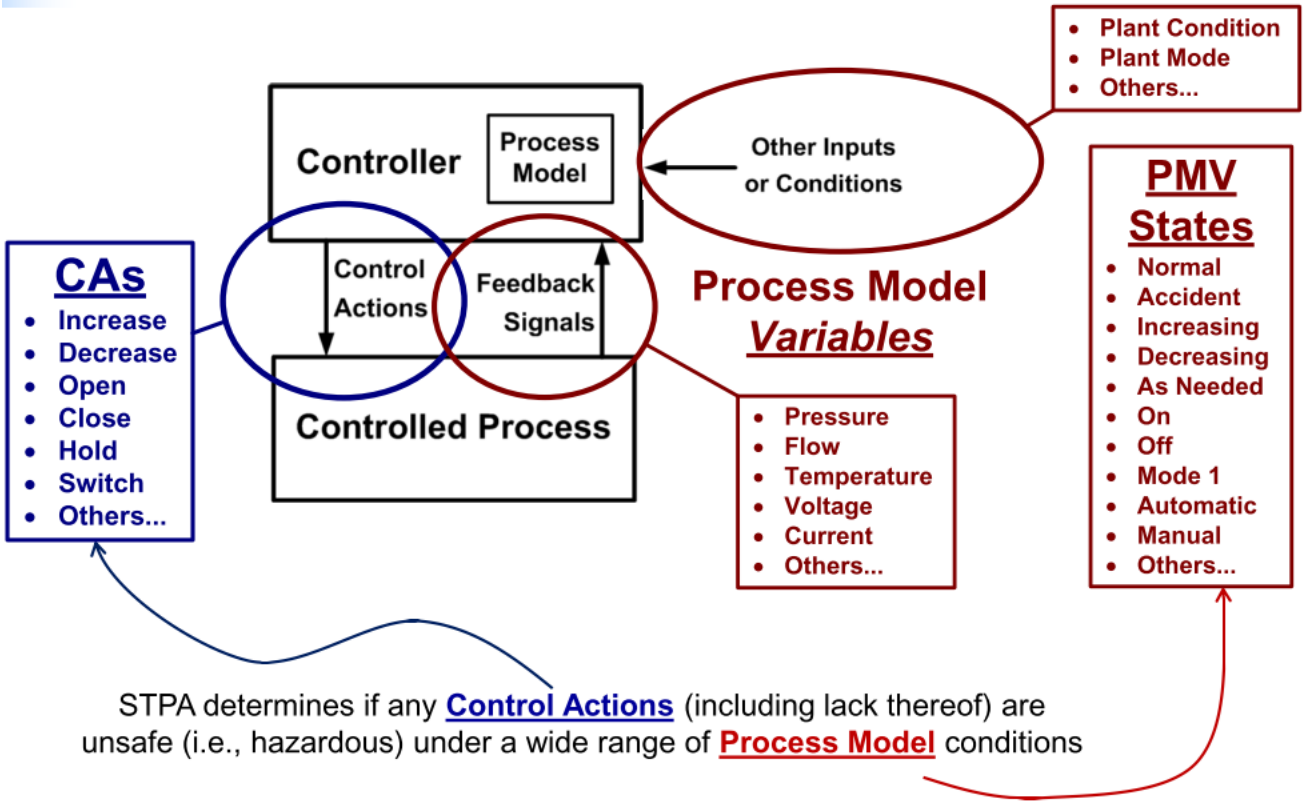






Hazard analysis 기법들 - STPA

- 작성 단계
  - Control loop



Hazard analysis 기법들 - STPA

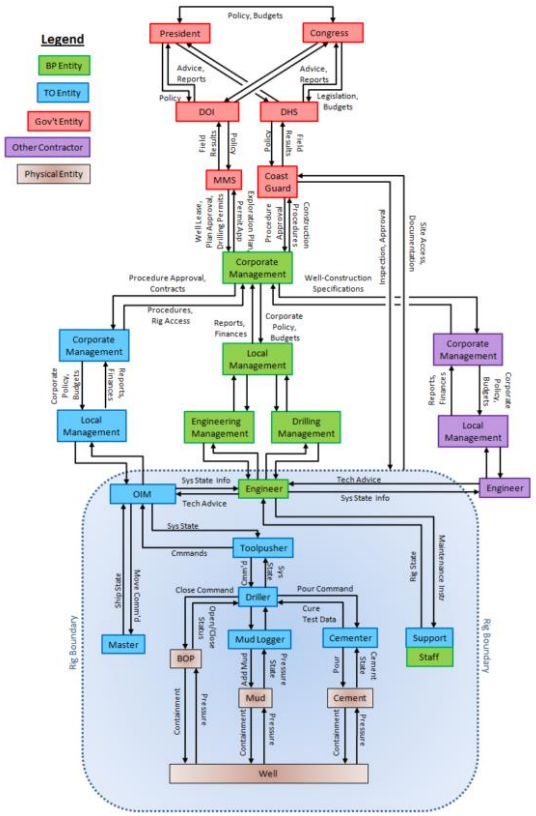
- 작성 단계
  - Unsafe control action category
    - 어떤 control action이 unsafe할 수 있는 경우를 4가지 카테고리로 나눔

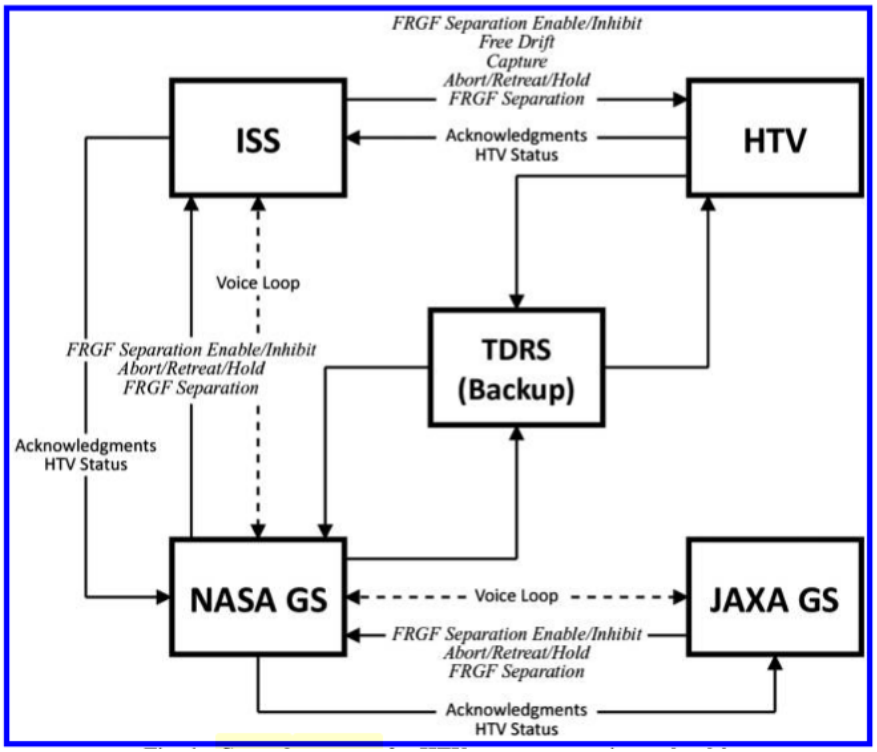
Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order causes hazard	Stopping too soon/applying too long causes hazard

Hazard: Loss of minimum separation				
Control Action	**Not Providing CA Causes Hazard**	**Providing CA Causes Hazard**	**Wrong Timing/Order of CA Causes Hazard**	**CA Stopped Too Soon/Applied Too Long**
Execute ITP		ITP executed when not approved ITP executed when ITP criteria are not satisfied ITP executed with incorrect climb rate, final altitude, etc.	ITP executed too soon before approval ITP executed too late after reassessment	ITP aircraft levels off above requested FL ITP aircraft levels off below requested FL

Hazard analysis 기법들 - STPA

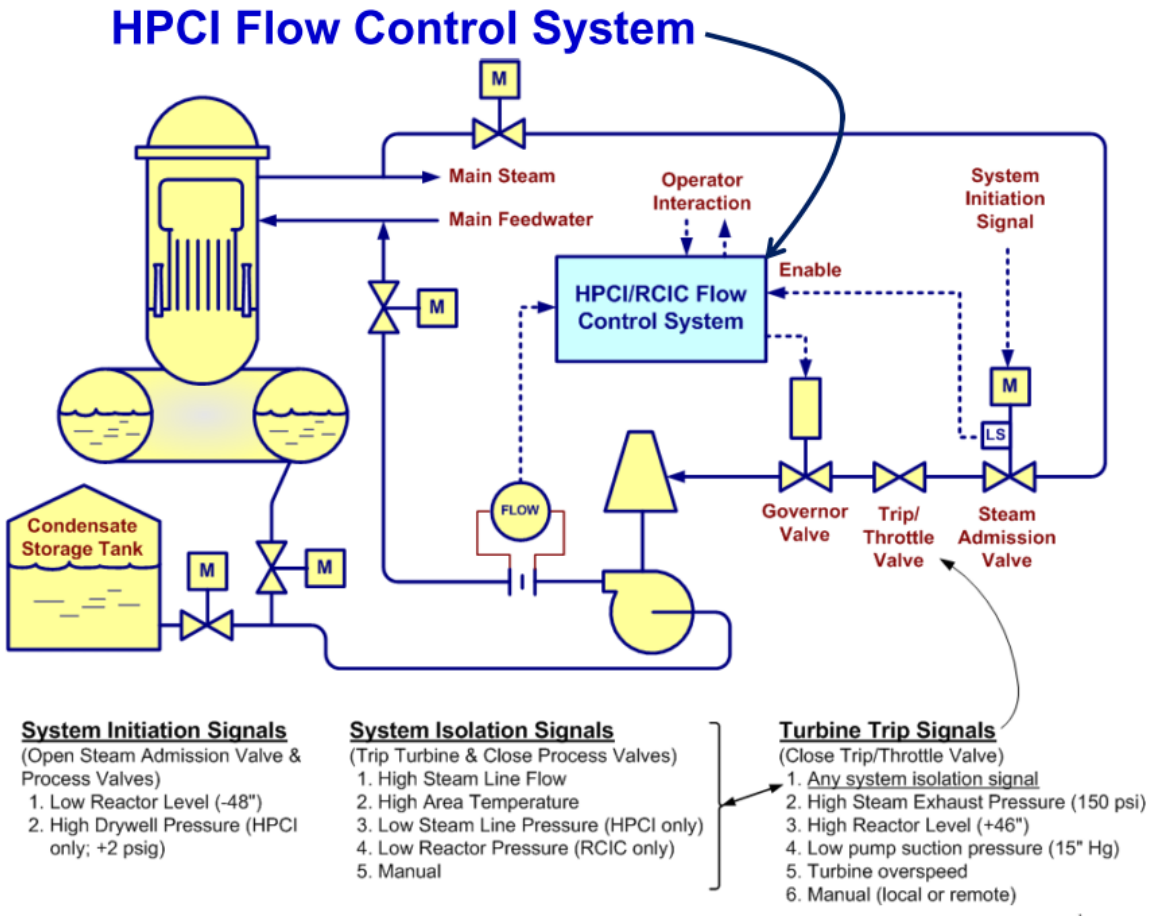
- 작성 단계
  - Control structure
    - 여러 개의 control loop를 합치는 것으로 만들어지며, 각 컴포넌트간의 동작을 나타낸 시스템의 설계도에 가까운 역할을 함.





Hazard analysis 기법들 - STPA

- 작성 단계



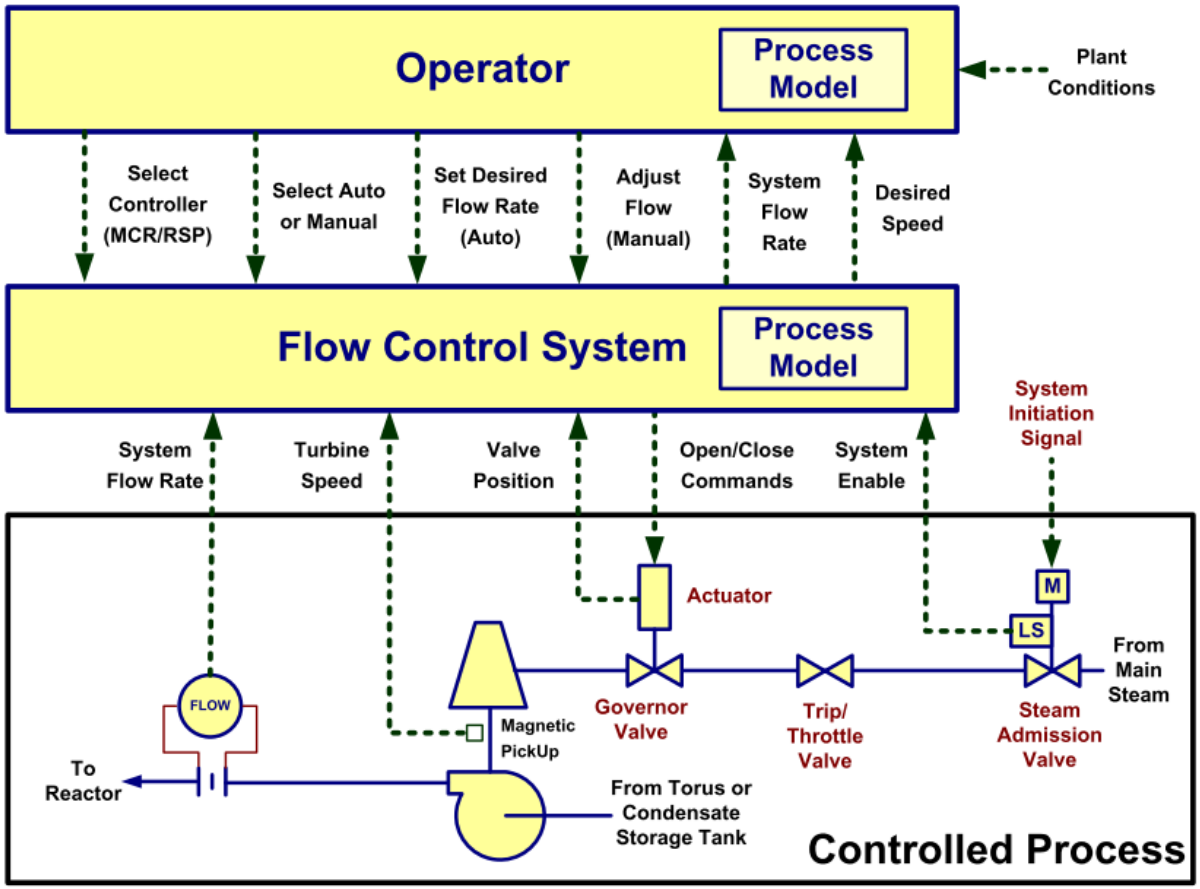
Hazard analysis 기법들 - STPA

- 작성 단계
  1. 시스템 레벨의 accident와 hazard, safety constraint의 식별

		Accidents				
		A1	A2	A3	A4	A5
Hazards		Radiation Exposure	Contaminated Enviroment	Equipment Damage	Injury or Death	Lost Generation
H1	Reactor Exceeds Limits			X		X
H2	Radioactive Material Release	X	X			
H3	Equipment Operated Beyond Limits			X	X	
H4	Inadvertent Equip. Operation During Maintenance				X	
H5	Reactor Shutdown					X

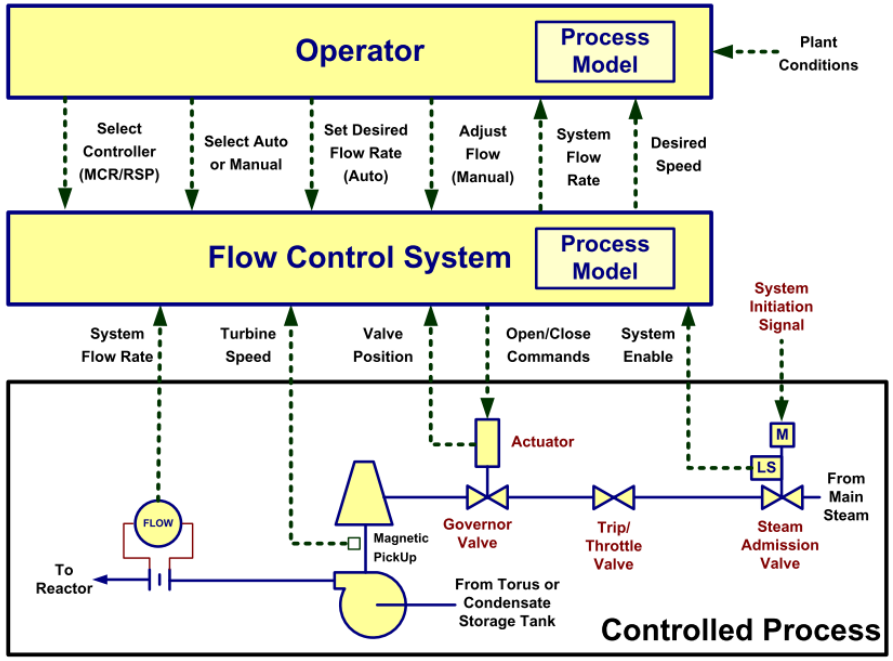
Hazard analysis 기법들 - STPA

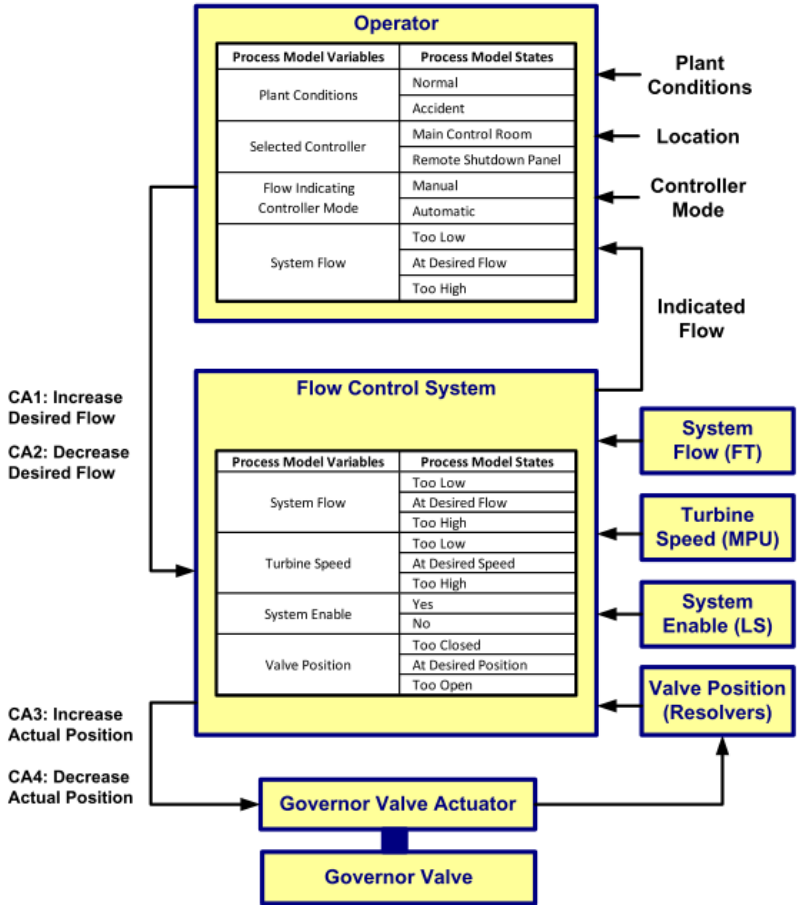
- 작성 단계
  2. Control structure의 구축



Hazard analysis 기법들 - STPA

- 작성 단계
  2. Control structure의 구축





Hazard analysis 기법들 - STPA

- 작성 단계
  3. Unsafe control action의 식별

Controller:	HPCI-RCIC Flow Control System		H1	Reactor Exceeds Limits
Control Action:	CA3	Increase Governor Valve Position	H2	Radioactive Release
			H3	Equipment Damage
Postulated Behavior:	Providing (the increase valve position command)		H4	Personnel Injury or Death
	(Is CA Behavior Hazardous?)		H5	Reactor Shutdown

Row	Process Model Variables					Analysis Results			
	PMV1 Plant Conditions	PMV2 Valve Position	PMV3 Turbine Speed	PMV4 System Flow	PMV5 System Enable	Is Situation Already Hazardous?	Is CA Behavior Hazardous?	Related Hazards	Comments (Situational Context)
1	Accident	Too open	Too high	Too high	Yes	Yes	Yes	H3	Leads to Rx overfill
2					No	Yes	No Response	H1, H2	Accident and no enable
3				Too low	Yes	Yes	Maybe	H3	Increase flow, but overspeed?
4					No	Yes	No Response	H1, H2	Accident and no enable
5				As needed	Yes	No	Yes	H3	Leads to Rx overfill
6					No	Yes	No Response	H1, H2	Accident and no enable
7			Too low	Too high	Yes	Yes	Yes	H3	Leads to Rx overfill
8					No	Yes	No Response	H1, H2	Accident and no enable
9				Too low	Yes	Yes	Maybe	H3	Increase flow, but valve damage?
10					No	Yes	No Response	H1, H2	Accident and no enable
11				As needed	Yes	No	Yes	H3	Leads to Rx overfill
12					No	Yes	No Response	H1, H2	Accident and no enable
13				Too high	Yes	Yes	Yes	H3	Leads to Rx overfill
14					No	Yes	No Response	H1, H2	Accident and no enable

Hazard analysis 기법들 - STPA

- 작성 단계
  3. Unsafe control action의 식별

Hazardous Control Actions										Hazard
Flow control system <u>provides</u> increase governor valve position (CA3) when:										
1	there is an accident	and valve position is	*	and turbine speed is	*	and system flow is	*	and system enable is	No[1]	H1, H2
2	there is an accident	and valve position is	too open or as needed	and turbine speed is	too high or as needed	and system flow is	*	and system enable is	Yes	H3
3	there is an accident	and valve position is	too closed	and turbine speed is	too high or as needed	and system flow is	*	and system enable is	Yes	H3
4	there is an accident	and valve position is	too closed	and turbine speed is	too low	and system flow is	too high or as needed	and system enable is	Yes	H3
5	there is <u>not</u> an accident	and valve position is	*	and turbine speed is	too high	and system flow is	too high	and system enable is	Yes[2]	H1
6	there is <u>not</u> an accident	and valve position is	*	and turbine speed is	too high	and system flow is	*	and system enable is	No[3]	H3
Flow control system <u>does not provide</u> increase governor valve position (CA3) when:										
7	there is an accident	and valve position is	*	and turbine speed is	*	and system flow is	too low	and system enable is	*[4]	H1, H2

Hazard analysis 기법들 - STPA

- 작성 단계
  4. Unsafe control action의 잠재 원인 식별

Hazard: Equipment Operated Beyond Limits (H3)
Controller: HPCI-RCIC Flow Control System
Hazardous Control Action No. 2: "Increase governor valve position" command is provided when: there is an accident and turbine speed is too high, regardless of system flow
Inadequate, Missing or Delayed Feedback
Enable signal sent to controller before there is a valid demand on HPCI/RCIC
enable provided when steam admission valve is not open (broken or misaligned LS)
steam admission valve commanded open when there is no demand on HPCI/RCIC (spurious ESFAS signal)
enable provided when steam admission valve is opened, but too late (misaligned LS or LS setpoint too high)
steam admission valve commanded open too late when there is a demand on HPCI/RCIC (ESFAS delay)
HPCI/RCIC pump flow rate signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution
Signal corrupted during transmission
sensor failure
sensor design flaw
sensor operates correctly but actual flow rate is outside sensor's operating range
fluid type is not as expected (water vs. steam?)
Governor valve position signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution
Problems with communication path
actual position is beyond sensor's range
sensor reports actuator position and it doesn't match valve position
sensor correctly reports valve position but position doesn't match assumed area/shape

Hazard analysis 기법들 - STPA

- 장점
  - Failure가 발생하지 않아도 컴포넌트간의 상호작용에서 발생할 수 있는 hazard를 찾아낼 수 있음.
- 단점
  - 경우의 수 조합이 너무 많아질 수 있음.
  - 자동화의 어려움.

Hazard analysis 기법들 - STPA

- 추가사항
  - Systems-Theoretic Accident Model and Processes (STAMP)
    - STPA는 System theory를 기반으로 한 Systems-Theoretic Accident Model and Processes (STAMP) 라고 하는 accident causality model을 사용함.
    - Accident causality model이란 hazard analysis 기법에서 accident가 어떻게 그리고 왜 발생하는지에 대해 생각하는 기본 개념을 말함.
    - STAMP는 Accident를 하나의 컴포넌트에서 발생하는 것이 아니라 전체 시스템의 control에서 발생하는 control problem으로 보고 시스템에 대한 safety constraint의 부족함에서 발생하는 것으로 봄.
  - Chain-of-Failure-Event causality model
    - Chain-of-event model이라고도 하며 기존의 HA 기법들은 이 모델을 기반으로 분석을 수행함.
    - Accident가 failure의 연쇄로 인해 발생하는 것이라고 생각하는 모델임.
    - Fault tree, HAZOP, FMEA 등 여러 기법들의 기초가 됨.

Hazard analysis 기법들 -
Software system safety engineering process

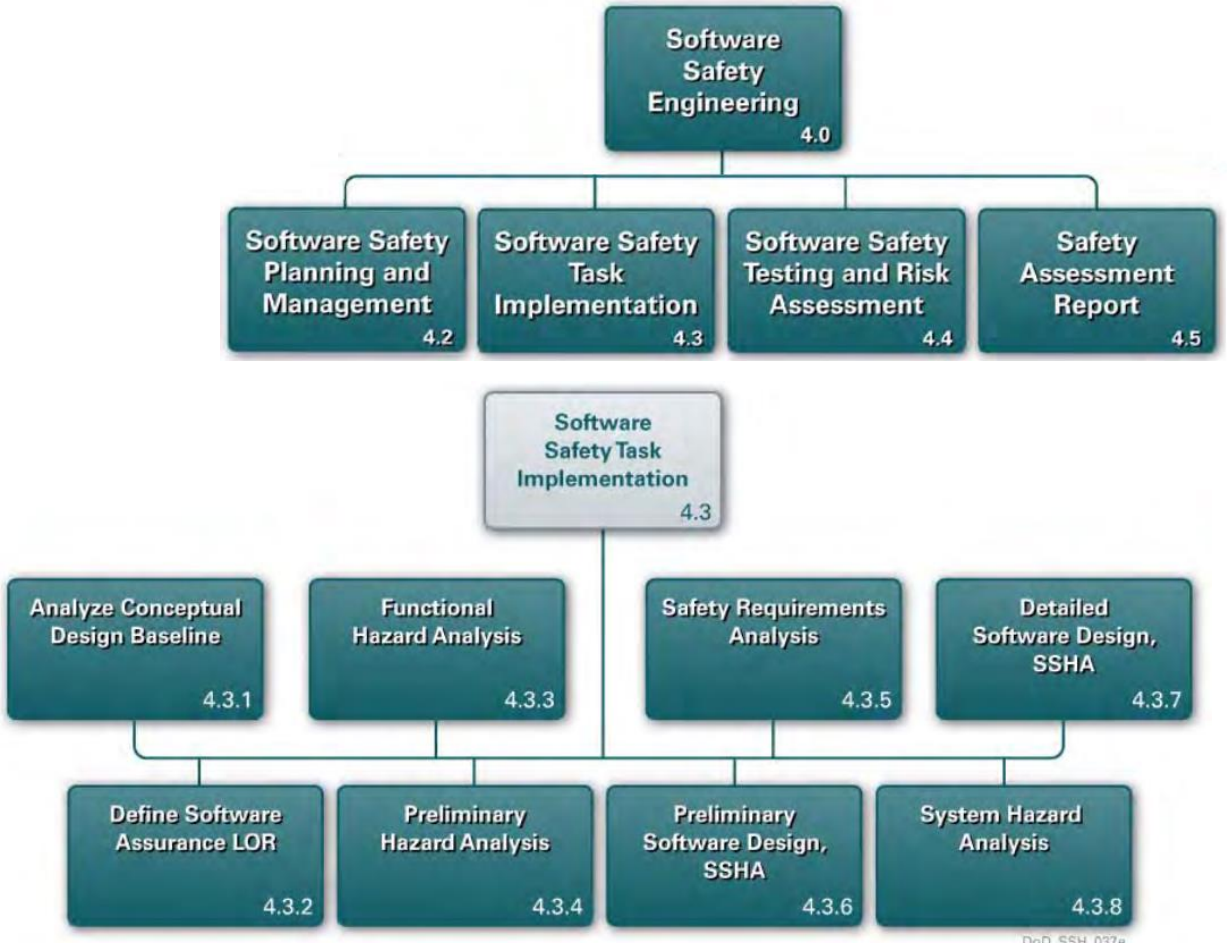
- 사용 이유
  - SW safety program은 system safety program, software development plan, program milestone과 통합되어 병렬적으로 진행되어야 하기 때문.

Hazard analysis 기법들 -
Software system safety engineering process

- 작성 단계
  1. 소프트웨어 안전 계획 수립 및 관리
  2. 소프트웨어 안전 과제 수행
     1. 개념 디자인 기초 분석
     2. 소프트웨어 보장 엄격성 기준 정의
     3. 기능적 위해 분석
     4. 초기 위해 분석
     5. 안전 요구사랑 분석
     6. 초기 소프트웨어 디자인의 서브시스템 위해 분석
     7. 세부 소프트웨어 디자인의 서브시스템 위해 분석
     8. 시스템 위해 분석
  3. 소프트웨어 안전 시험 및 위험 평가
  4. 안전 평가 보고

Hazard analysis 기법들 -
Software system safety engineering process

- 작성 단계



Issue

Issue

- FPGA 이전의 디자인 단계에서 hazard analysis를 수행하는 것에 대한 issue 존재.
- NuSCR이라고 하는 formal specification을 이용해 FPGA 상위 단계에서 내부의 컨트롤 소프트웨어의 디자인을 수행함.
- STPA를 기반으로 하여 SW의 formal specification을 사용하는 것으로 SW의 operation이 system level의 hazard에 어떤 영향을 미치는지에 대한 분석을 수행.
- 해당 과정을 위한 프로세스를 만들어서 제시.

Issue

- STPA를 이용한 시스템 소프트웨어 동작의 위해도 분석 개념도