東京工業大学
Tokyo Institute of Technology

Rationalized Alarm Logic Design based on PHA

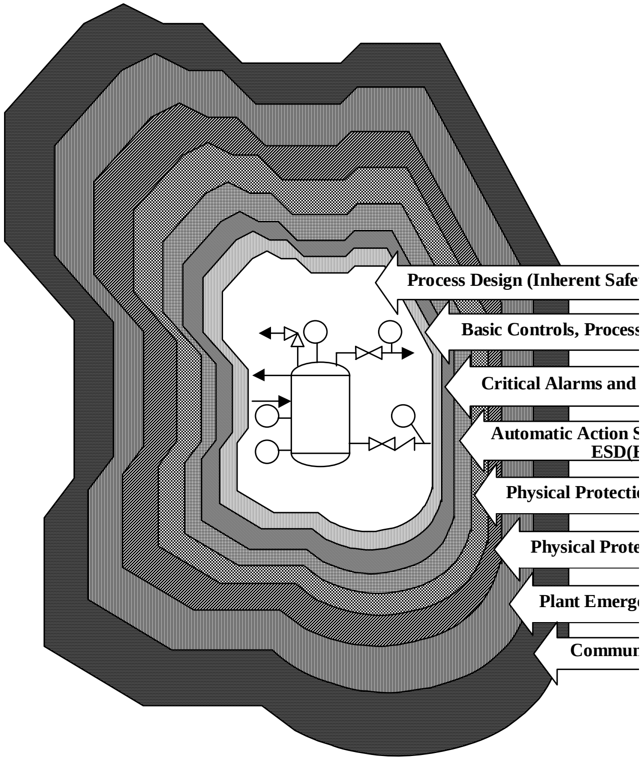
Yu Shazawa, Tokyo Institute of Technology

Yukiyasu Shimada, National Institute of Occupational safety and Health

Tetsuo Fuchino, Tokyo Institute of Technology

IPL: Independent Protection Layers

(AIChE CCPS (1992))



IPL	Function
1	Inherent Safety
2	BPCS
3	Critical Alarms
4	Safety Instrumented System
5	Relief Devices
6	Physical Protection
7	Emergency Response

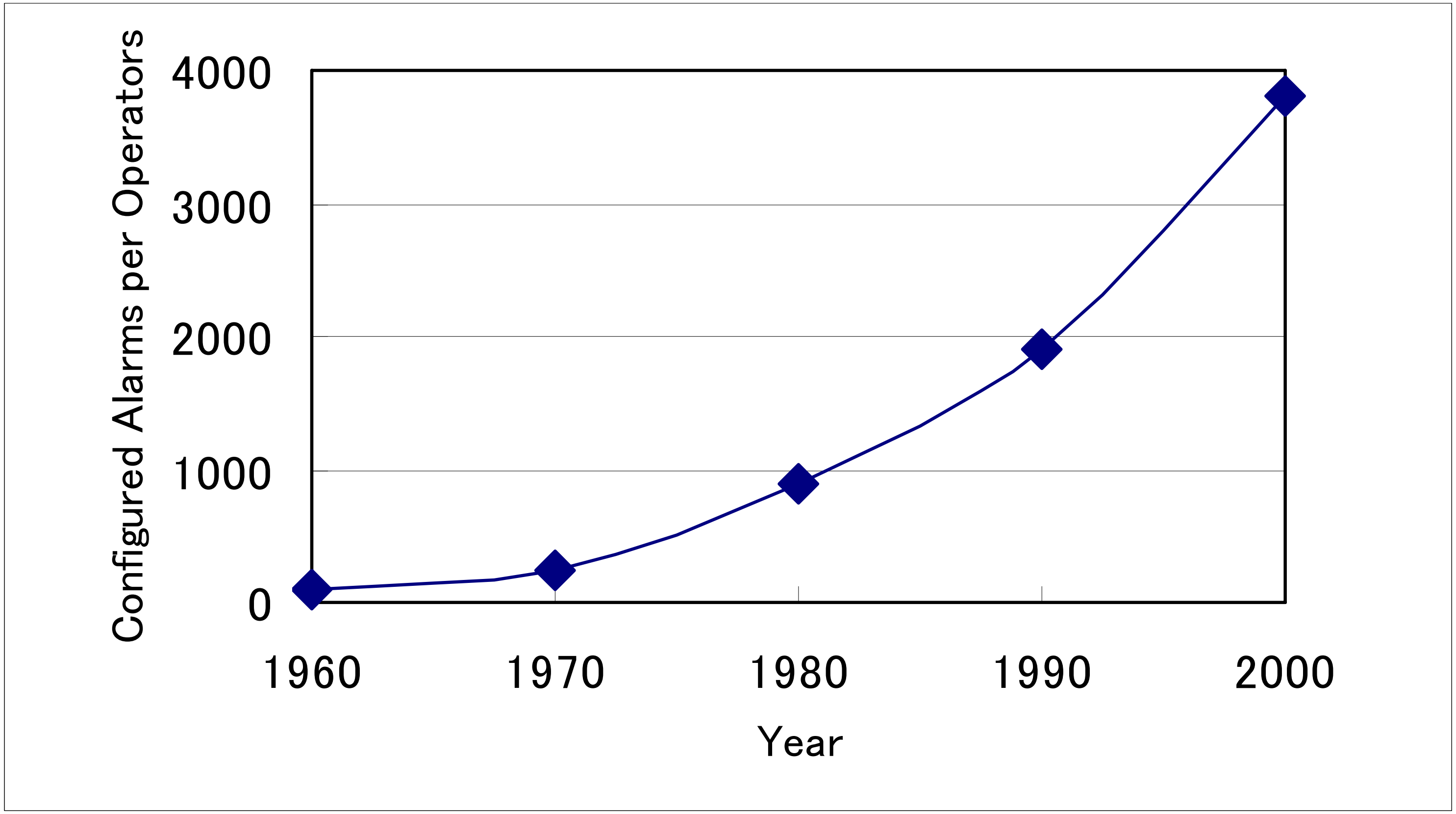
Function of Alarm System

- A process alarm is a mechanism for informing a operator of an abnormal process condition for which **an operator action is required.**
- The operator is alerted **in order to prevent or mitigate process upset and disturbances.**

ISA, Alarm Management(2007)

→ Needless Alarms for operator's action must not be configured.

Number of alarms has been increasing drastically



ISA, Alarm Management(2007)

Too many alarms for operators to take correct action.

How are Alarms designed ?

Process Design Phase **Safety Design**

R&D → Test of Hazardous Materials
Bench Scale testing

Equipment Planning → Preliminary Hazard A

Outline of Alarm System are decided

Basic Design

Detailed Design

Safety Equipment Design
BPCS, Relief Valves, Proce
Interlock System, etc.

Additional Alarms are decided

Process Hazard Analysis (PHA)
HAZOP,FMEA,FTA etc.

The current design doesn’t consider the feasibility of operator responses

How does the procedure have to be improved?

To design Alarms which can complete responses

1. operator responses have to be clearly defined before alarm logics are determined.

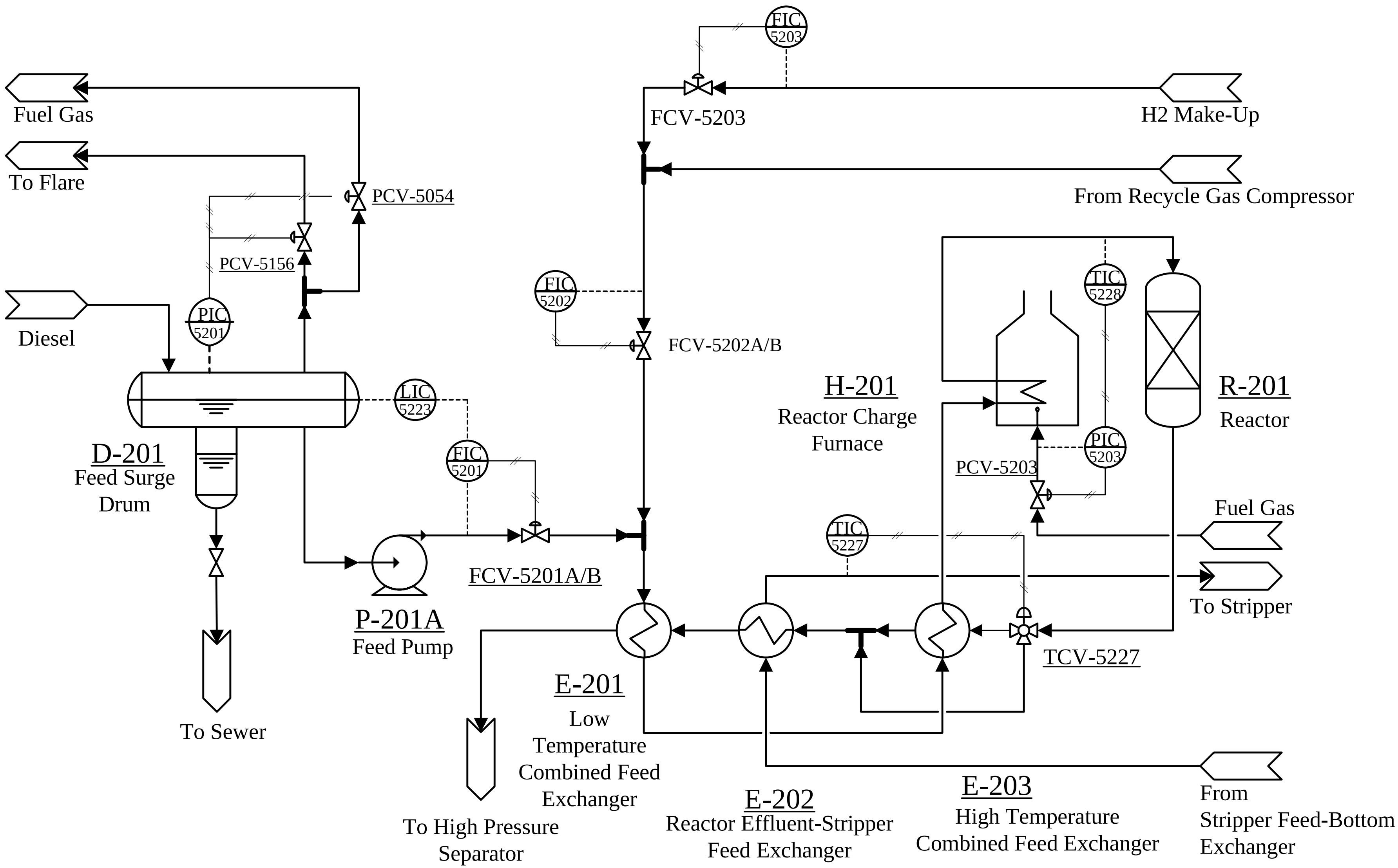
2. The feasibility of operator responses depends on

   - if there is enough time to respond.
   - if operators can judge correct actions.

Alarm system design must be consistent with PHA.

We developed the design method based on HAZOP.

PFD of HDS process around Reactor

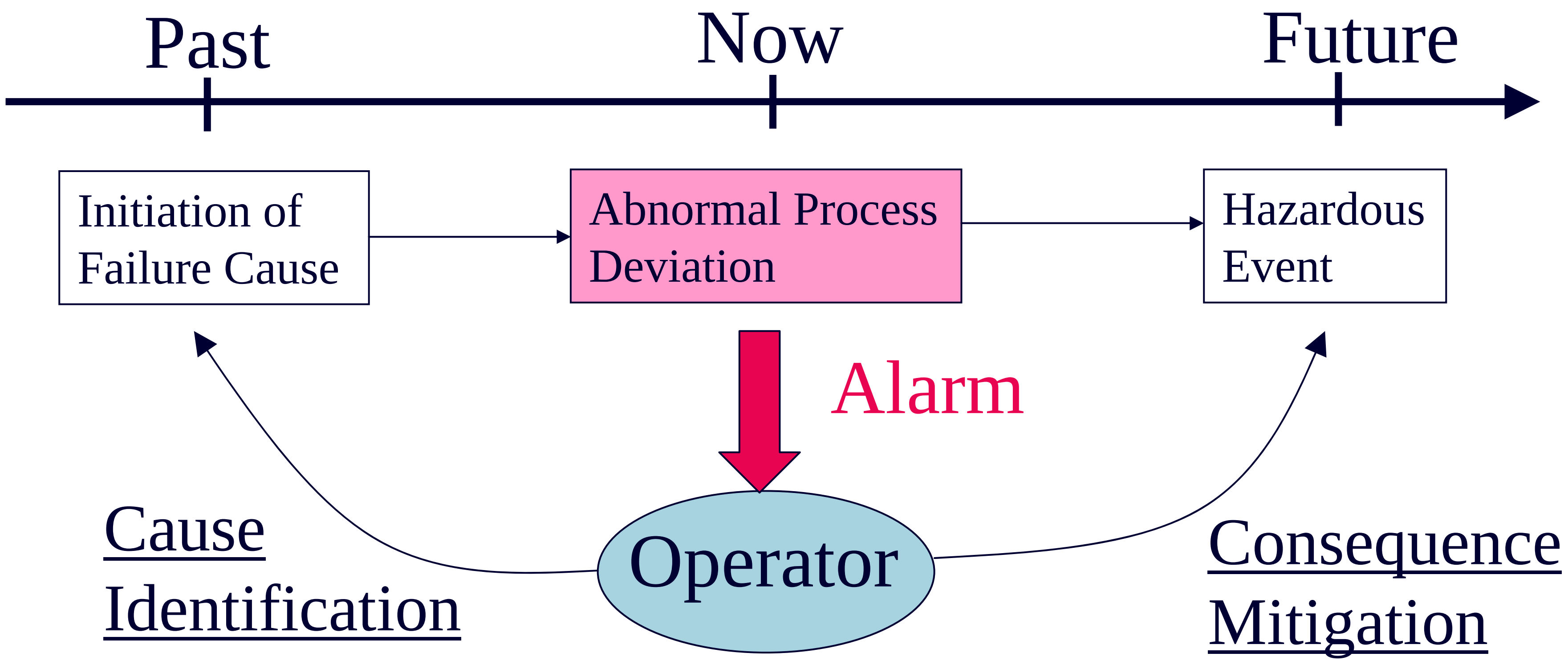


A part of HAZOP

Deviation	Potential Causes	No	Consequences	No	Mitigation
No Flow	Mechanical failure of Feed Pump (P-201S)	1	Level of Feed Surge Drum(D-201) rises and overflows. If inflow from upstream continues, There can be inflow to flare line. Process malfunction	1	Back-up Pump (P201A)
			Reverse flow to D-201 through Pump mini flow line. Hydrogen can also reverse to D-201.	2	Back-up Pump
			Furnace tube is overheated because Feed oil to Reactor Charge furnace(H-201) is lost and there is only hydrogen flow inside. If this continues long time, tube ruptures and fire break out inside H-201	3	a.P201A b.BPCS (TIC-5228)
			Desulfuration in Reactor(R-201) is stopped because of lack of Feed Oil	4	P201A
			Insufficient heat exchange in Reactant Effluent Feed Exchange(E-202) causes malfunction in Stripper (outside of this node)	5	a.P201A b.BPCS (TIC-5227)
			Level of High Pressure Separator lowers and process malfunction occurs	6	P-201A

17 potential causes are analyzed in HAZOP.

Responses can be separated into two groups



Responses to solve root causes ➡ **Past incident**

Responses to mitigate Consequences ➡ **Future incident**

Responses can be separated into two groups

(1) Responses to solve root causes

(2) Responses to mitigate consequences

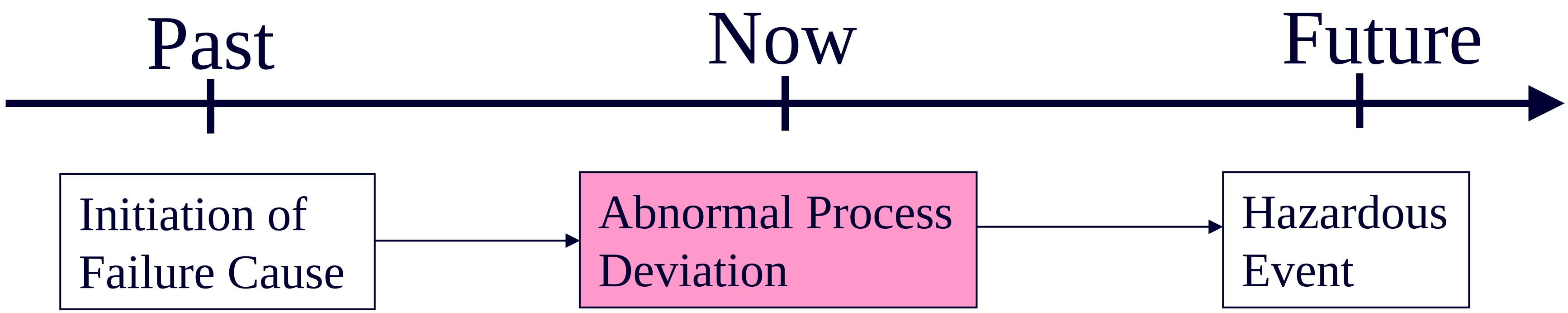
Example of HAZOP

Deviation	Potential cause	Consequence
No Flow	Mechanical Failure of Feed Pump	Stop of Desulfuration in reactor

(1) (2)

Design separate alarm logic for each group of operator responses.

Why is it better to separate?



- Alarm Logics for consequence mitigation

  One-to-One relationship between Response and Alarm Logic is possible.

- Alarm Logics for cause identification

  One-to-One relationship between Response and Alarm Logic may be impossible.

Procedure of Alarm Logic Design based on HAZOP

a. Design of Alarm Logics for consequence mitigation

1. Produce Alarm Logic Design Base (ALDB) Sheet.
2. Prepare Alarm Priority Grid (APG).
3. Output the list of Alarm Logics for consequence mitigation.

b. Design of Alarm Logics for cause identification

1. Decide a tentative pair of Alarm Logics for cause identification.
2. Analyze the possibility of alarm activation by Event Tree Analysis (ETA)-based method.
3. Check whether the tentative pair is acceptable with Alarm Matrix

Preparation for Alarm Logic Design Base Sheet

HAZOP isn't applicable form to design Alarm Logic.

Transform HAZOP into ALDB Sheet.

Rearrange HAZOP so that propagation of process deviation can be understood.

- "Possible Impact "
- "Intermediate Deviation."

Add necessary information to HAZOP to prioritize each Alarm.

- Maximum Available response time.
- Severity of Possible Impact.

Classification of MART and Severity

MART (Maximum Available Response Time)

Rank	Definition
Insufficient	Insufficient time to respond
Immediate	There is time to respond, but immediate actions are necessary
Short	There is time to respond, but not enough
Long	There is enough time to respond

Severity

Rank	Definition
None	No loss
Minor	Plant operation is possible if impact occurs
Major	Plant operation is impossible if impact occurs
Severe	(More severe result is assigned to 'Severe')

Example of ALDB sheet

HAZOP

Deviation	Potencial cause	Consequence
No Flow	Mehchanical Failure of Feed Pump	Furnace tube is overheated because of Feed loss. If this continue long time, tube rupture and fire will happens.

Alarm Logic Design Base Sheet

Potential cause	First Deviation	Intermediate Deviation	Possible Impact	MART	Severity
Mechanical Failure of Feed Pump	No Flow	High temperature at furnace tube	tube rupture and fire	Short	Severe

(APG) Alarm Priority Grid

APG can determine whether alarm is needed, and evaluate priority ranks of each alarm logic.

(Priority) = (Severity) × (MART)

Alarm Priority Grid

		Severity			
		None	Minor	Major	Severe
Response Time	Long	No Alarm	Low	Low	High
	Short		Low	High	High
	Immediate		High	Emergency	Emergency
	Insufficient		High	No Alarm,but SIS is necessary	

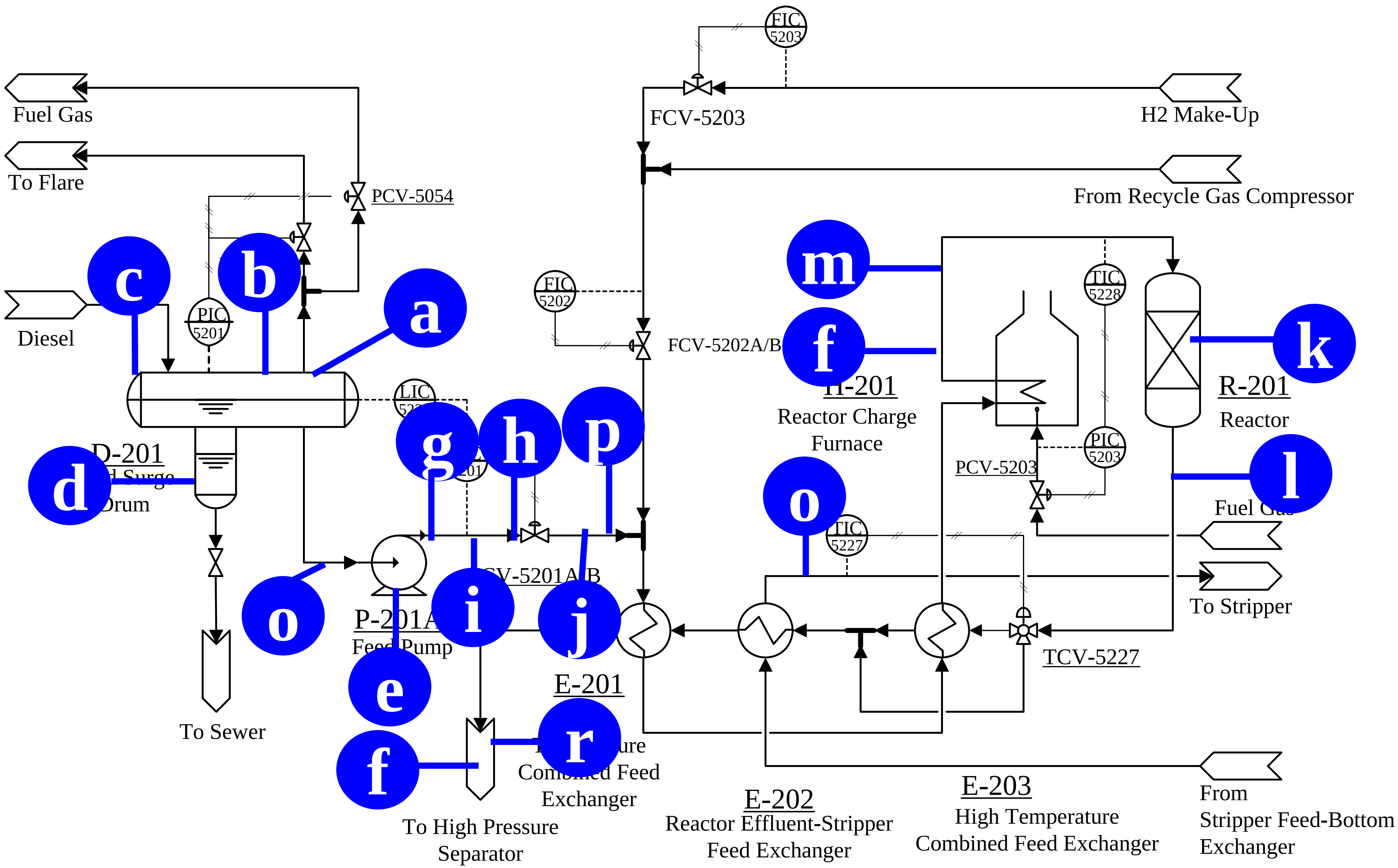
Production of AL list for Consequence mitigation

Code	Place	Parameter	Priority
a	D-201	Level High	Low
b	D-201	Level Low	High
c	D-201	Pressure High	Low
d	D-201 Boot	Level High	Low
e	Feed Pump Line	Pressure High	Low
f	Reactor Charge Furnace Tube	Temperature High	Emergency
g	[illegible]	[illegible]	[illegible]
h	[illegible]	[illegible]	[illegible]
i	[illegible]	[illegible]	[illegible]
j	[illegible]	[illegible]	[illegible]
k	[illegible]	[illegible]	[illegible]
l	[illegible]	[illegible]	[illegible]
m	Reactor Charge Furnace Tube	Temperature Low	Low
n	D-202	Level Low	Low
o	Feed Line to T-202 from E-202	Temperature Low	Low
p	Both Lines of FCV-5201A/B	More Flow	Low
q	Start-up Bypass	Flow Detection	Low
r	Exit of C-204	Temparature High	Low

18 Alarm Logics

for consequence mitigation.

PFD of HDS process around Reactor



Procedure of Alarm Logic Design based on HAZOP

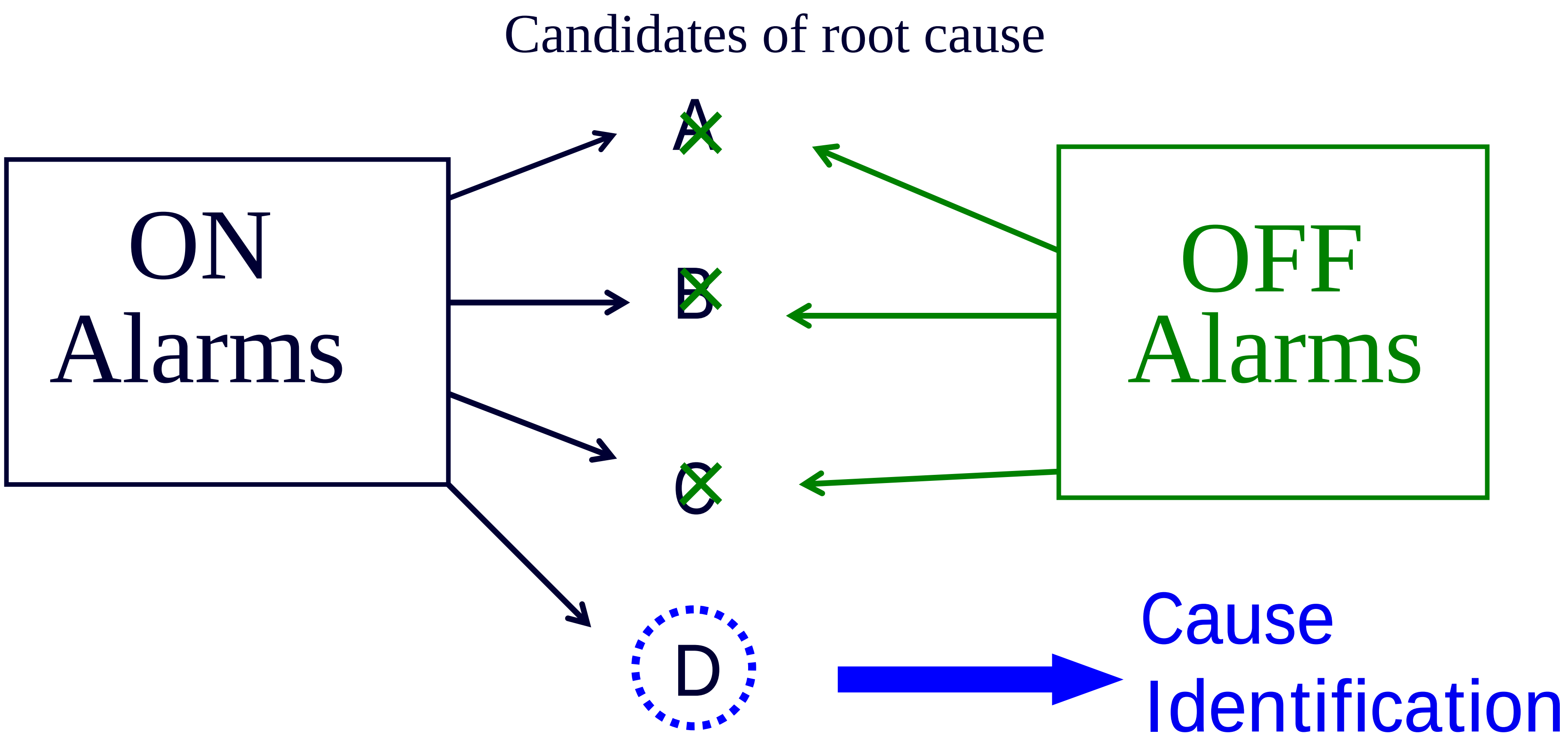
a. Design of Alarm Logics for consequence mitigation

1. Produce Alarm Logic Design Base (ALDB) Sheet.
2. Prepare Alarm Priority Grid (APG).
3. Output the list of Alarm Logics for consequence mitigation.

b. Design of Alarm Logics for cause identification

1. Decide a tentative pair of Alarm Logics for cause identification.
2. Analyze the possibility of alarm activation by Event Tree Analysis (ETA)-based method.
3. Check whether the tentative pair is acceptable with Alarm Matrix

The approach to identify root causes



Operators identify causes by combination of ON-Alarms and OFF-Alarms.

Design procedure of ALs for cause identification

Step1: Decide a tentative pair of Alarm Logics to detect occurrence of each cause.

Step2: Analyze which alarm has possibility of activation under each abnormal situation.

Step3: Check whether it is possible to uniquely identify each root cause. If impossible, go back to Step1.

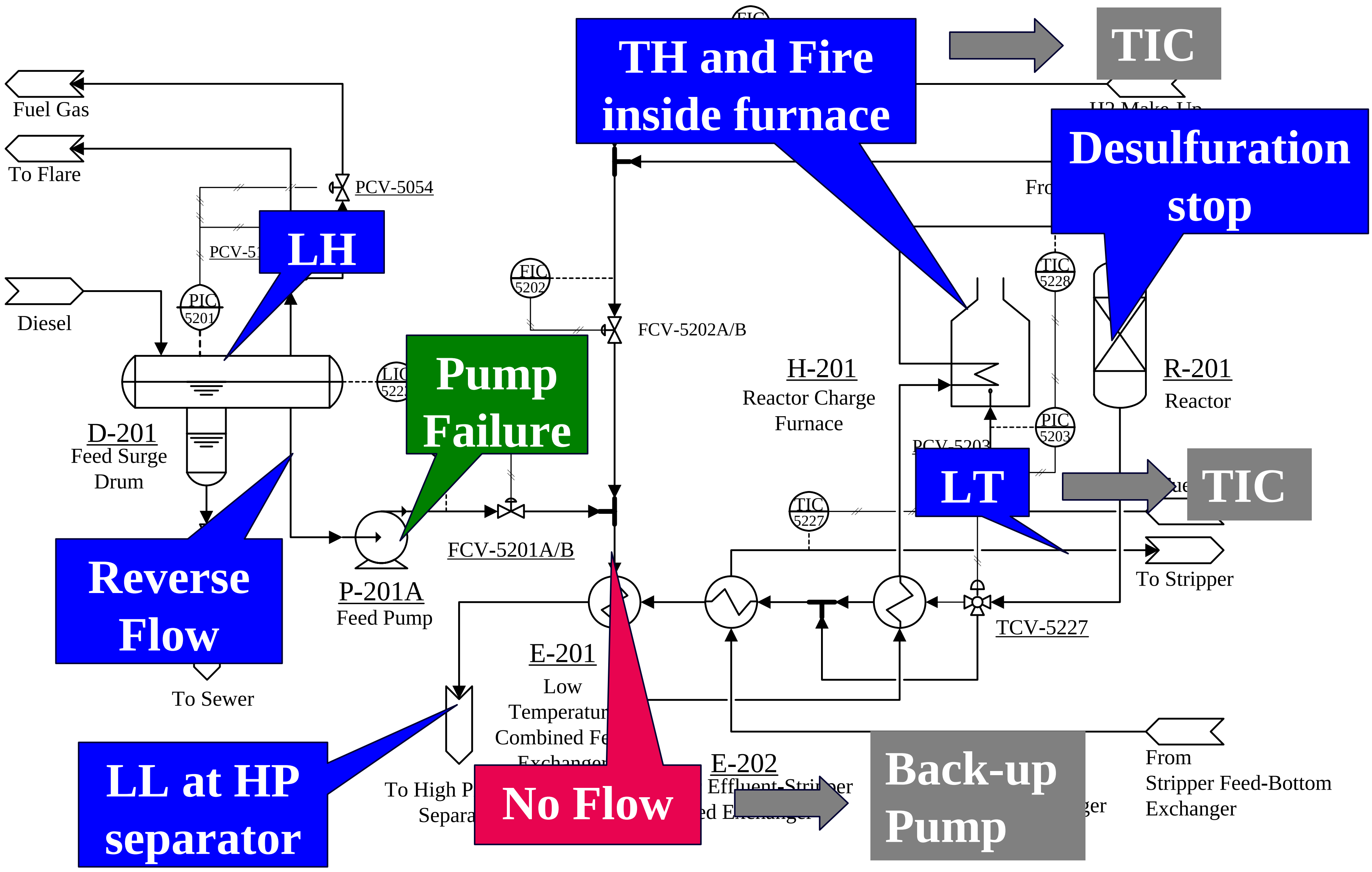
Step1:Decide a tentative pair of Alarm Logics

Assume the occurrence of each potential cause one-by-one ,and decide Alarm Logic individually .

Repeat the change of this pair until uniquely identification become possible at Step3 .

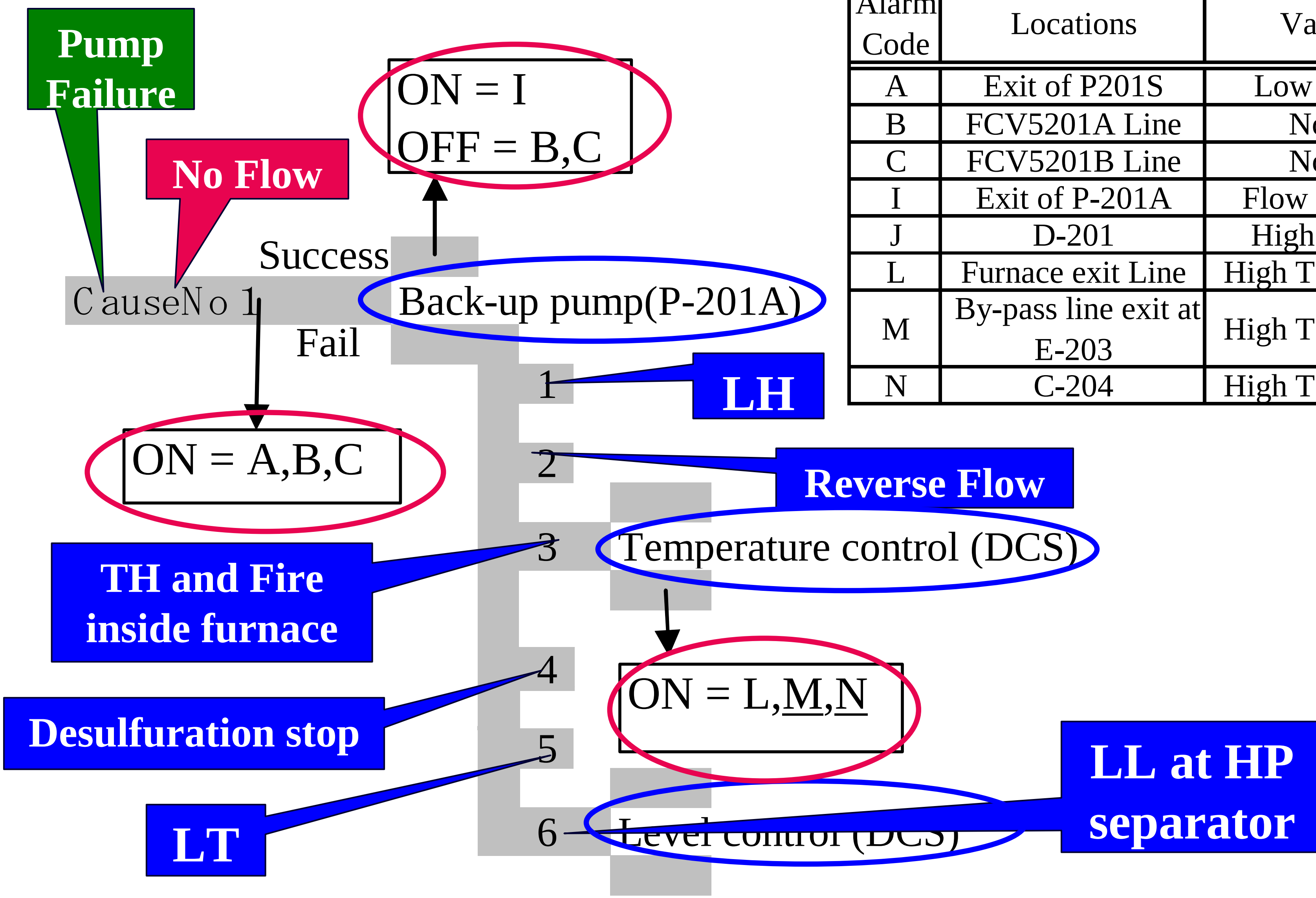
Example

Step2:Event Tree Analysis for Alarm Logic Design



Step2:Event Tree Analysis for Alarm Logic Design

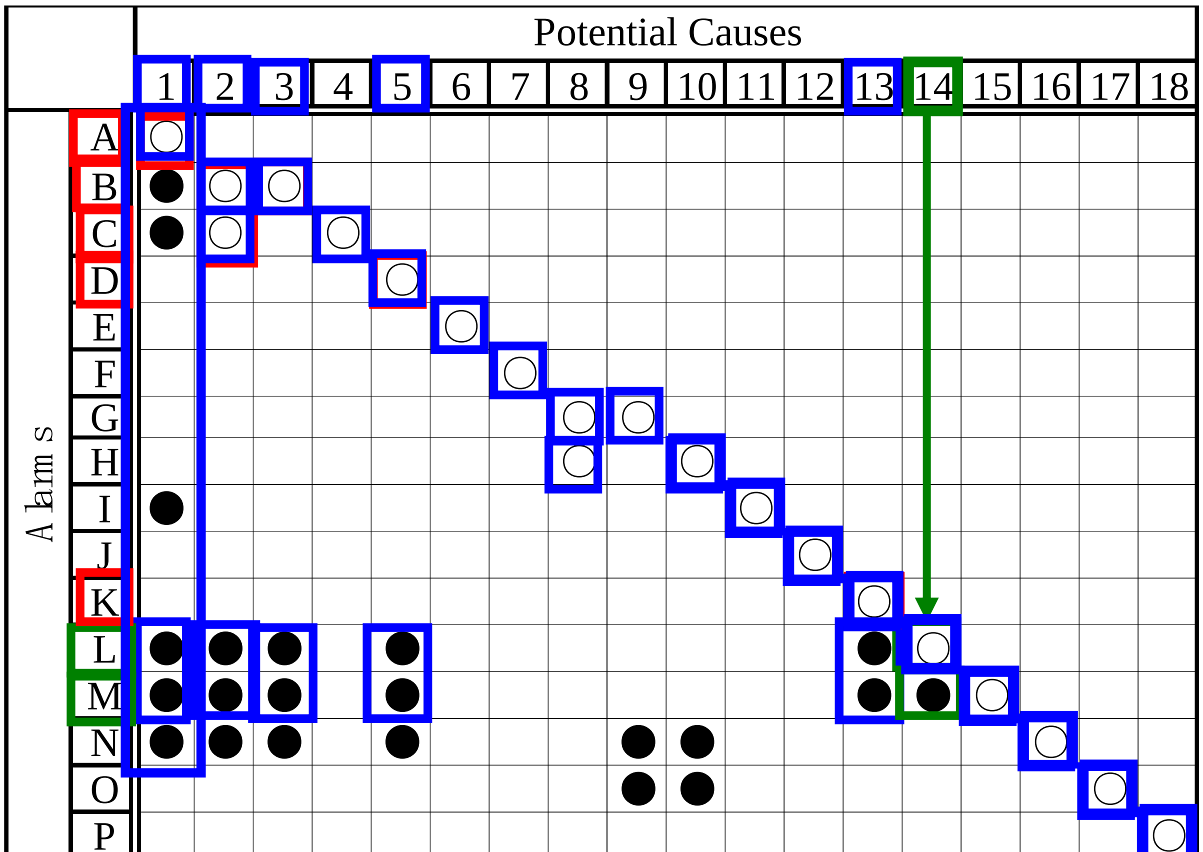
Alarm Code	Locations	Variables
A	Exit of P201S	Low Pressure
B	FCV5201A Line	No flow
C	FCV5201B Line	No flow
I	Exit of P-201A	Flow Detectoin
J	D-201	High Pressure
L	Furnace exit Line	High Temperature
M	By-pass line exit at E-203	High Temperature
N	C-204	High Temperature



Step3:Alarm Matrix

○ = Alarms which appear ahead of first branch and are never canceled on ETA

● = the other alarms except the above alarms



ON	OFF
L	A,BC, D,K

Cause Identification

Alarm Logic List for Cause Identification

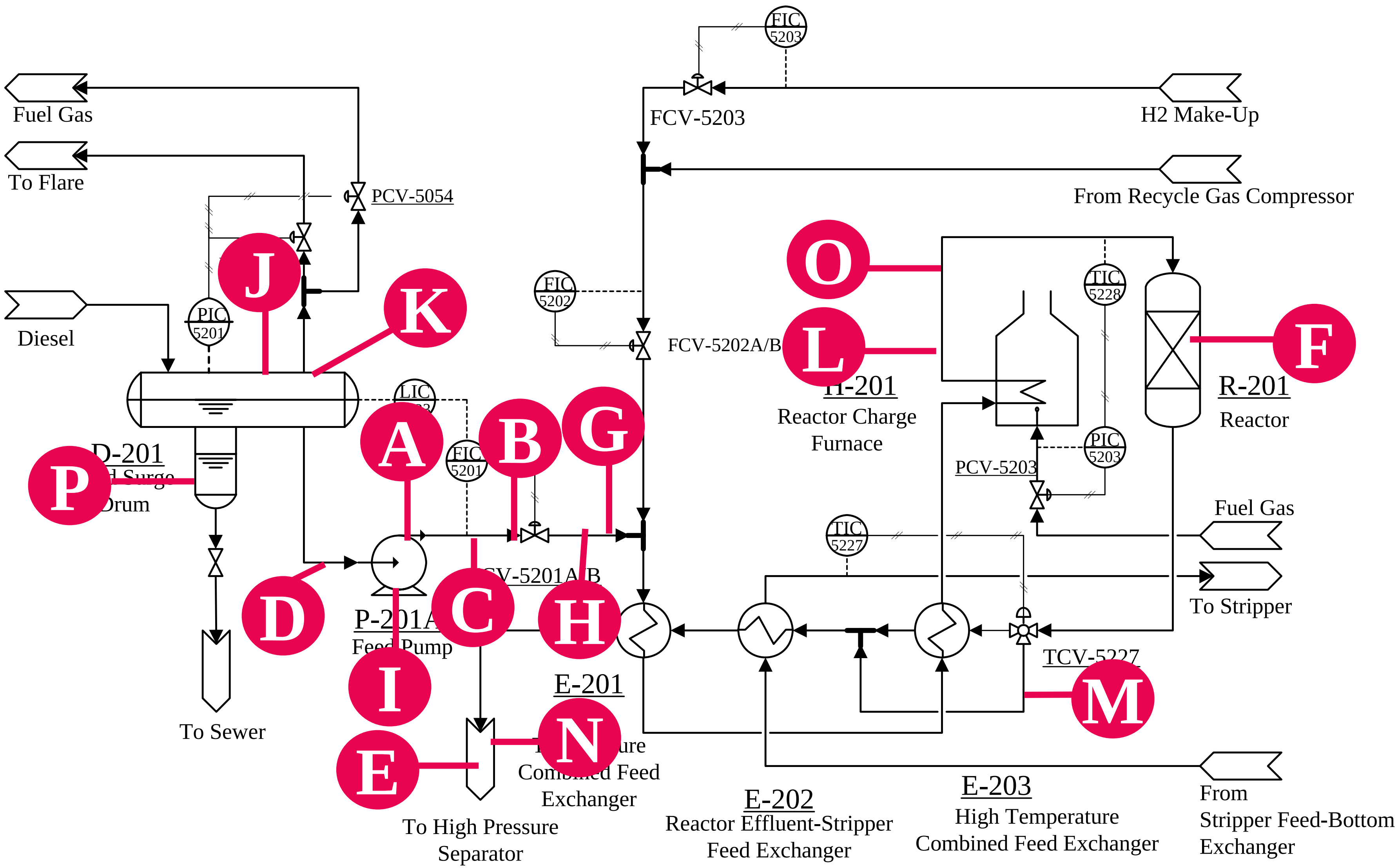
Alarm Logic List

Alarm Code	Locations	Variables
A	Exit of P201S	Low Pressure
B	FCV5201A Line	No flow
C	FCV5201B Line	No flow
D	Start-up bypass	Flow Detectoin
E	C-204	Stop of Water injection
F	Reactor(R-201)	Pressure difference High
G	FCV-5201A Line	More flow
H	FCV-5201B Line	More flow
I	Exit of P-201A	Flow Detectoin
J	D-201	High Pressure
K	D-201	Low Pressure
L	Furnace exit Line	High Temperature
M	By-pass line exit at E-203	High Temperature
N	C-204	High Temperature
O	Furnace exit Line	Low Temperature
P	Boot interface at D201	Level High

Evidence of Cause Identification

Cause No.	ON-Alarm	OFF-Alarm
1	A	
2	B,C	A
3	B	A,C
4	C	A,B
5	D	
6	E	
7	F	
8	G,H	
9	G	
10	H	
11	I	A
12	J	
13	K	
14	L	A,B,C,D,K
15	M	A,B,C,D,K,L
16	N	A,B,C,D,G,H
17	O	G,H
18	P	

PFD of HDS process around Reactor



Conclusion

- We proposed a new method of Alarm Logic Design based on HAZOP.
- We separately design two groups of Alarm Logics; One is for cause identification, the other is for consequence mitigation.
- We illustrated this method through the case study of HAZOP result for HDS process around Reactor.

Appendix

Rearrangement of HAZOP information

Pick out "Possible Impact" and "Intermediate Deviation" from each "Consequences" in HAZOP.

Possible Impact

The concrete process state which may lead to some loss.

Intermediate Deviation

Process variable deviation between first deviation and Possible Impact. This can be expressed with the same term as first deviation.

Rearrangement of HAZOP information

HAZOP

Deviation	Potencial cause	Consequence
No Flow	Mehchanical Failure of Feed Pump	Furnace tube is overheated because of Feed loss. If this continue long time, tube rupture and fire will happens.

Alarm Logic Design Base Sheet

Potential cause	First Deviation	Intermediate Deviation	Possible Impact	MART	Severity
Mechanical Failure of Feed Pump	No Flow	High temperature at furnace tube	tube rupture and fire		

Classification of MART

Evaluate MART (Maximum Available Response Time) and Severity to each possible Impact.

MART (Maximum Available Response Time)

the time within which operators can take actions to prevent Possible Impact from happening if there are no other safety equipments.

Severity

How severe Possible Impact is if it become realize.

Classification of MART and Severity

HAZOP

Deviation	Potencial cause	Consequence
No Flow	Mehchanical Failure of Feed Pump	Furnace tube is overheated because of Feed loss. If this continue long time, tube rupture and fire will happens.

Alarm Logic Design Base Sheet

Potential cause	First Deviation	Intermediate Deviation	Possible Impact	MART	Severity
Mechanical Failure of Feed Pump	No Flow	High temperature at furnace tube	tube rupture and fire	Short	Severe

(APG) Alarm Priority Grid

APG can evaluate whether alarm is needed, and priority ranks to each alarm.

(Priority) = (Severity) × (MART)

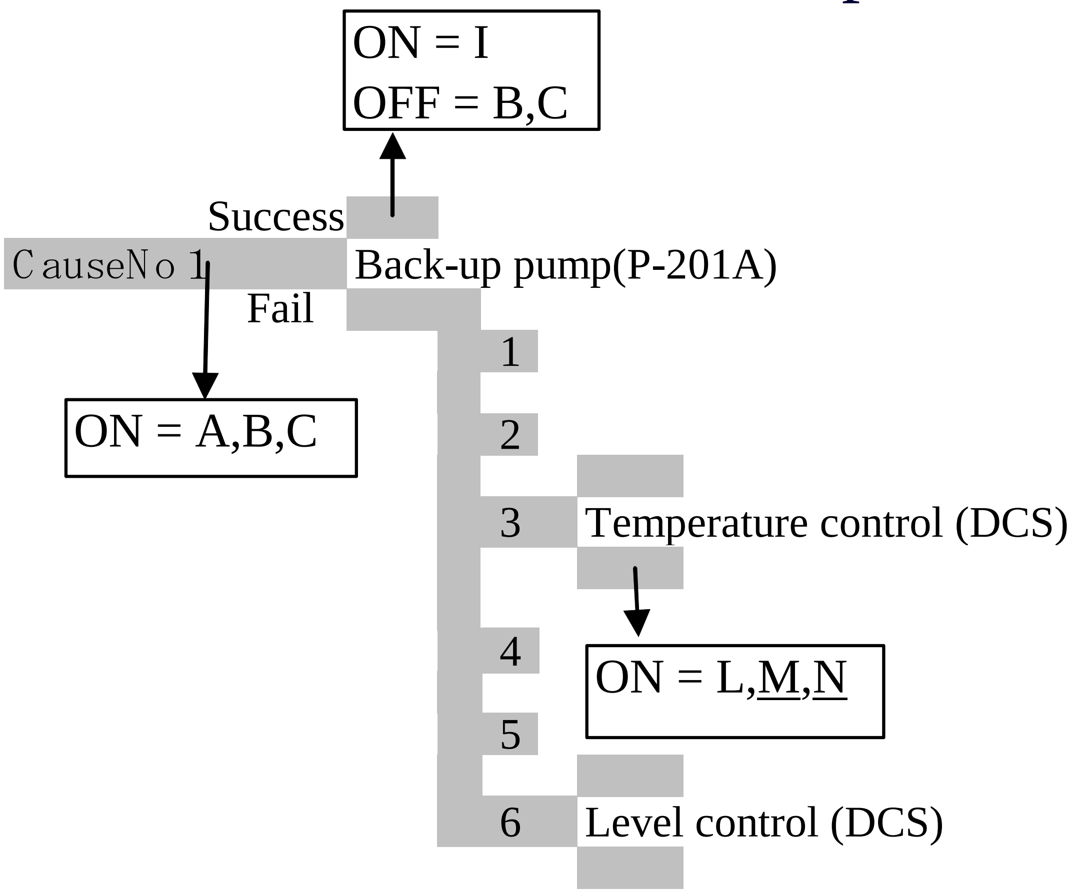
		Severity			
		None	Minor	Major	Severe
Response Time	Long	No Alarm	Low	Low	High
	Short		Low	High	High
	Immediate		High	Emergency	Emergency
	Insufficient		High	No Alarm,but SIS is necessary	

Safety Interlock System with **adequate Safety Integrity Level(SIL)** must be implemented

Step3:Alarm Matrix

○ = Alarms which appear ahead of first branch and are never canceled

● = the other alarms except ON-Alarms



○	●
A	B,C,L, M,N