Comparative Analysis of Hazard and Operability Study (HAZOP) and Systems Theoretic Process Analysis (STPA)

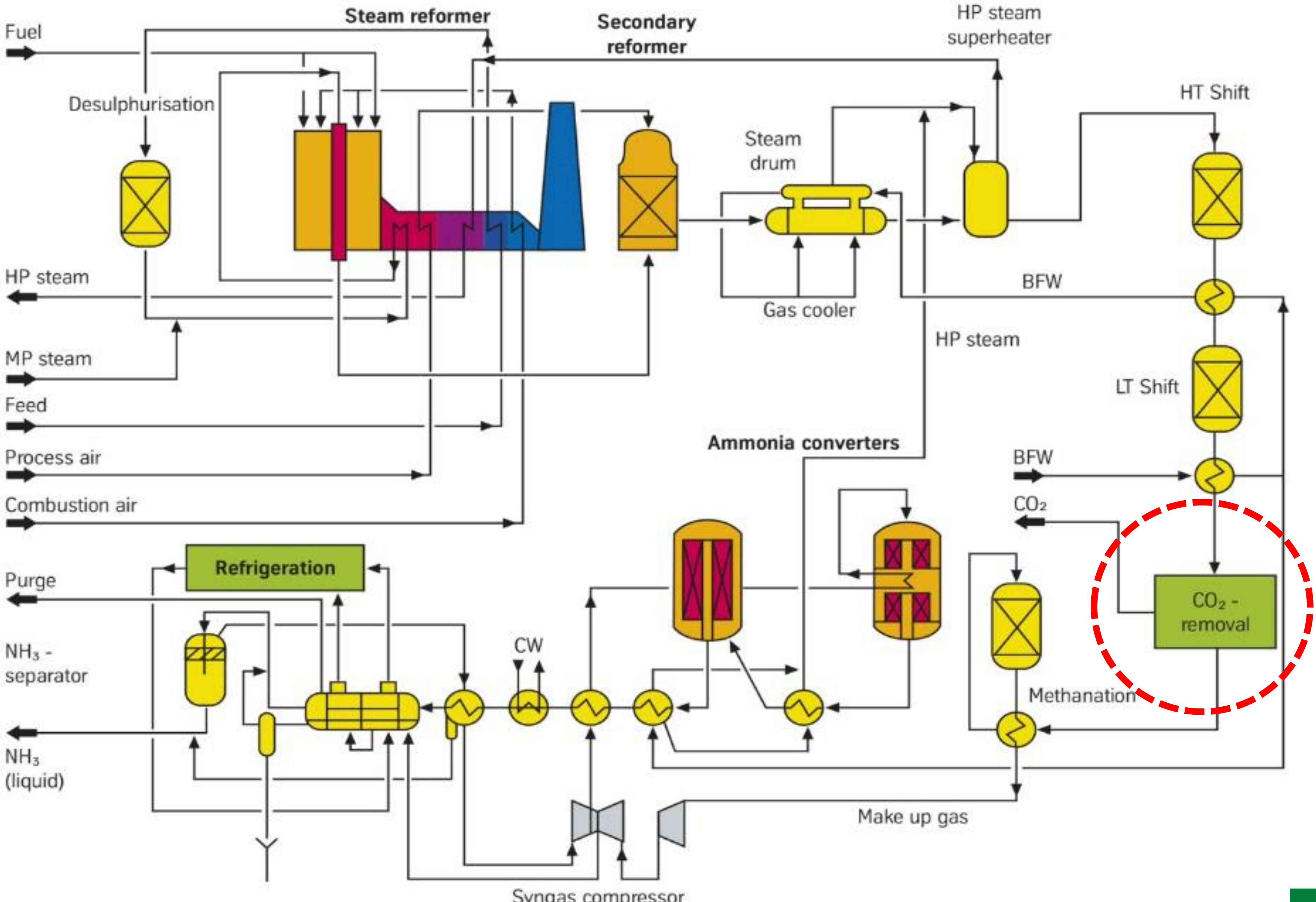
Faisal Jamal
Manager - Corporate HSE & TS, Fatima Fertilizer Company Limited, Pakistan

Dr. John P. Thomas
Scientist - Department of Aeronautics and Astronautics, MIT, USA

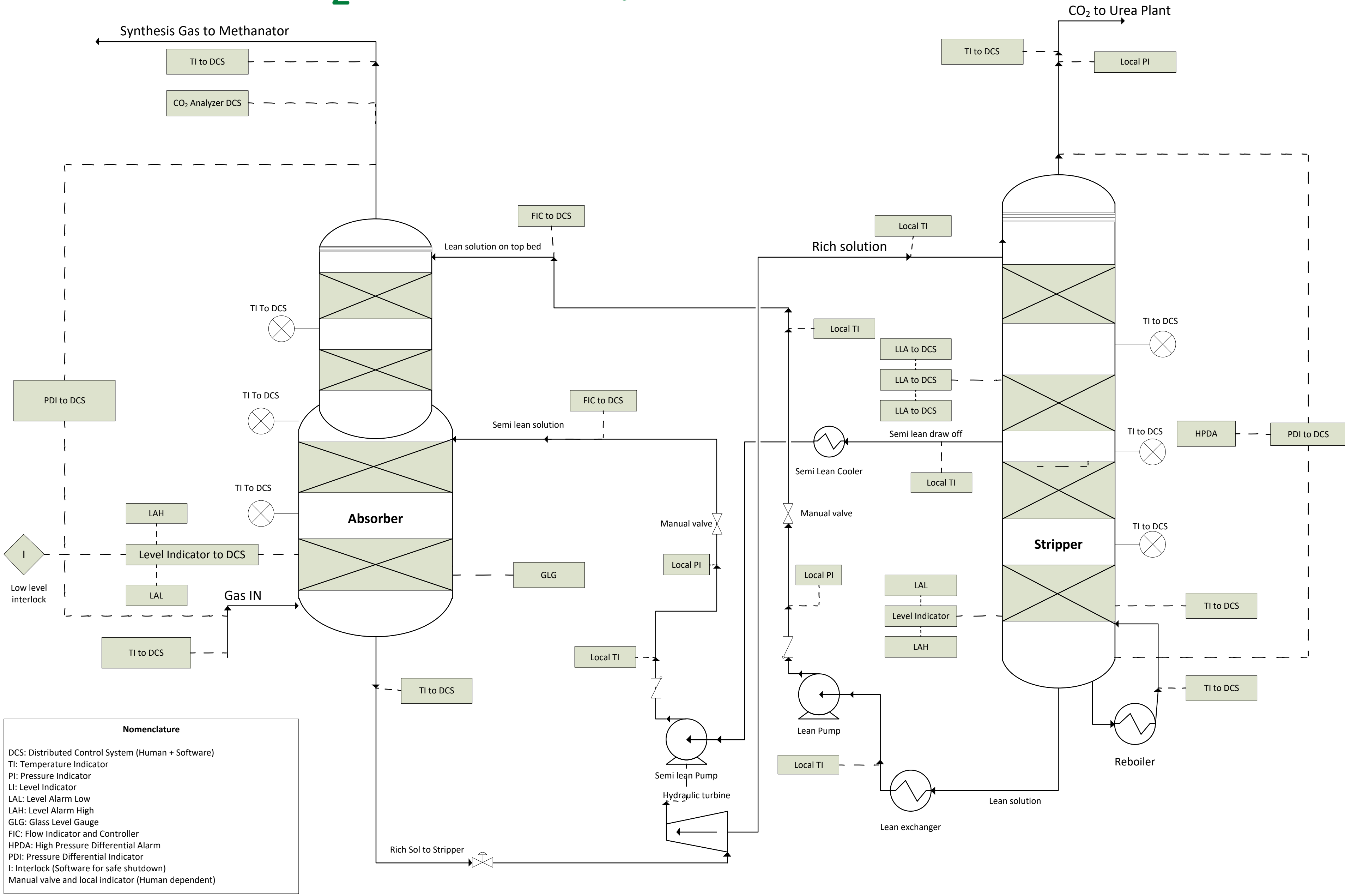
Preamble

- Fatima Fertilizer Company Limited (FFL) - Fatima Group's flagship manufacturing facility. Annual fertilizer production 1.3 MT.
- DuPont Process Safety Management (PSM) Excellence Level-4. More than 55 Million man-hours without a Lost Time Injury (LTI).
- An endeavor to establish a comparison between STPA and current and established risk assessment techniques in the process industry - HAZOP.
- Looked at past 30 years' incidents in Ammonia plants using published info.
- Selected the complex CO_2 Removal System - includes human, machine and software interactions.
- This system's HAZOP was conducted by an experienced and qualified team maintaining high quality as per HAZOP methodology.
- An incident occurred on this HAZOP-ed system due to a missing control logic - not identified during HAZOP.

Ammonia Production Process Flow



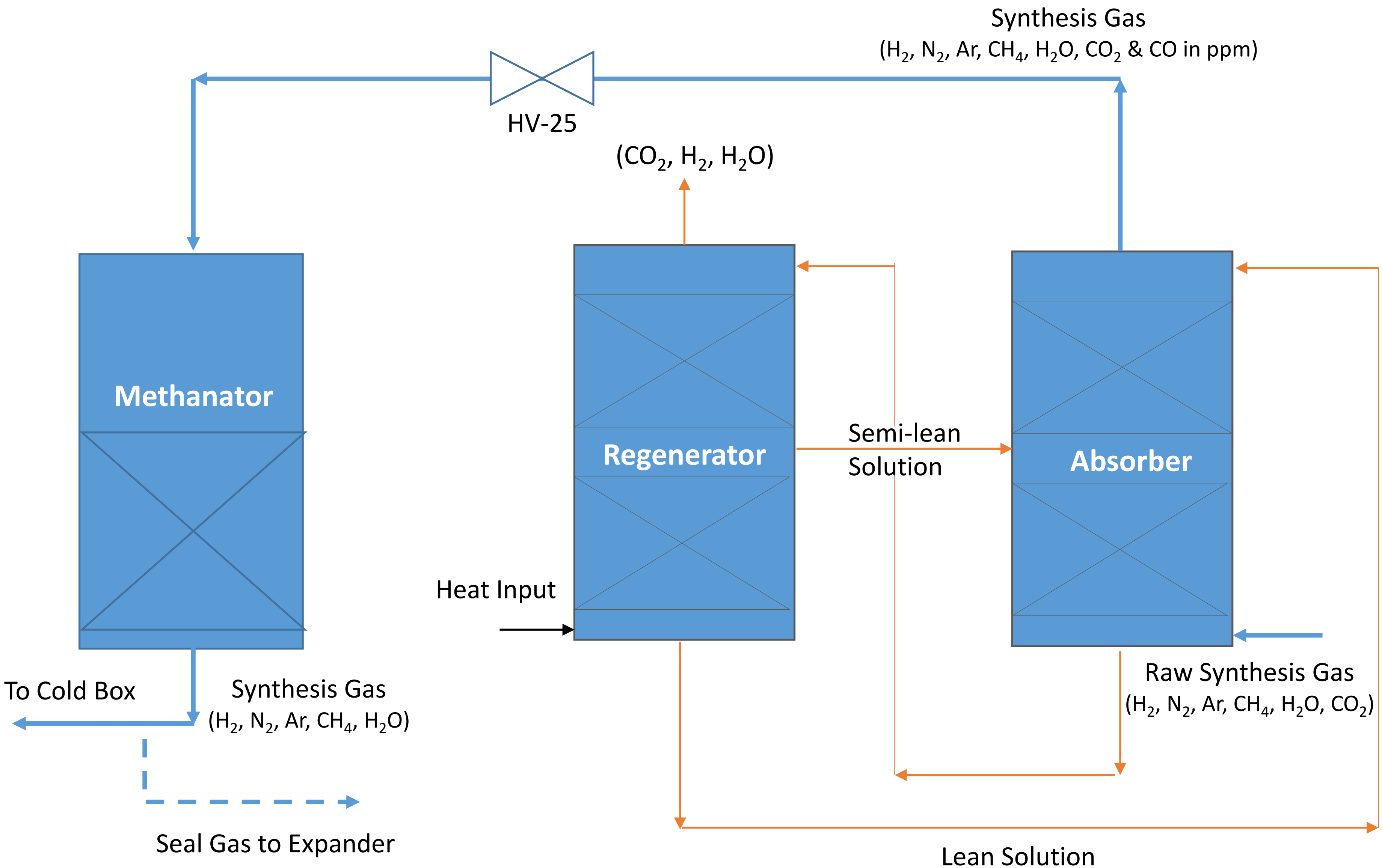
CO_2 Removal System Process Flow



Nomenclature

DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)

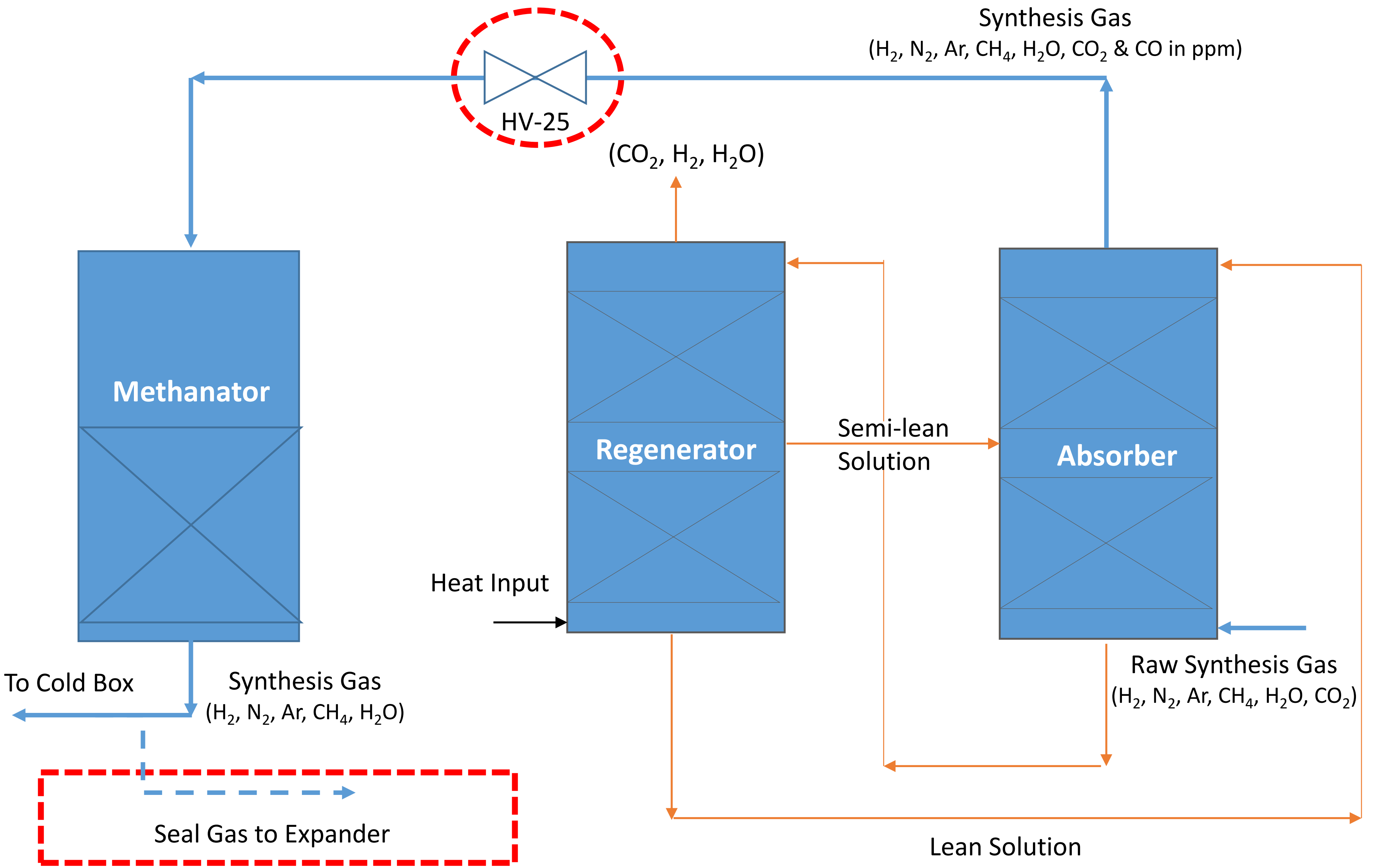
CO_2 Removal System Process Flow



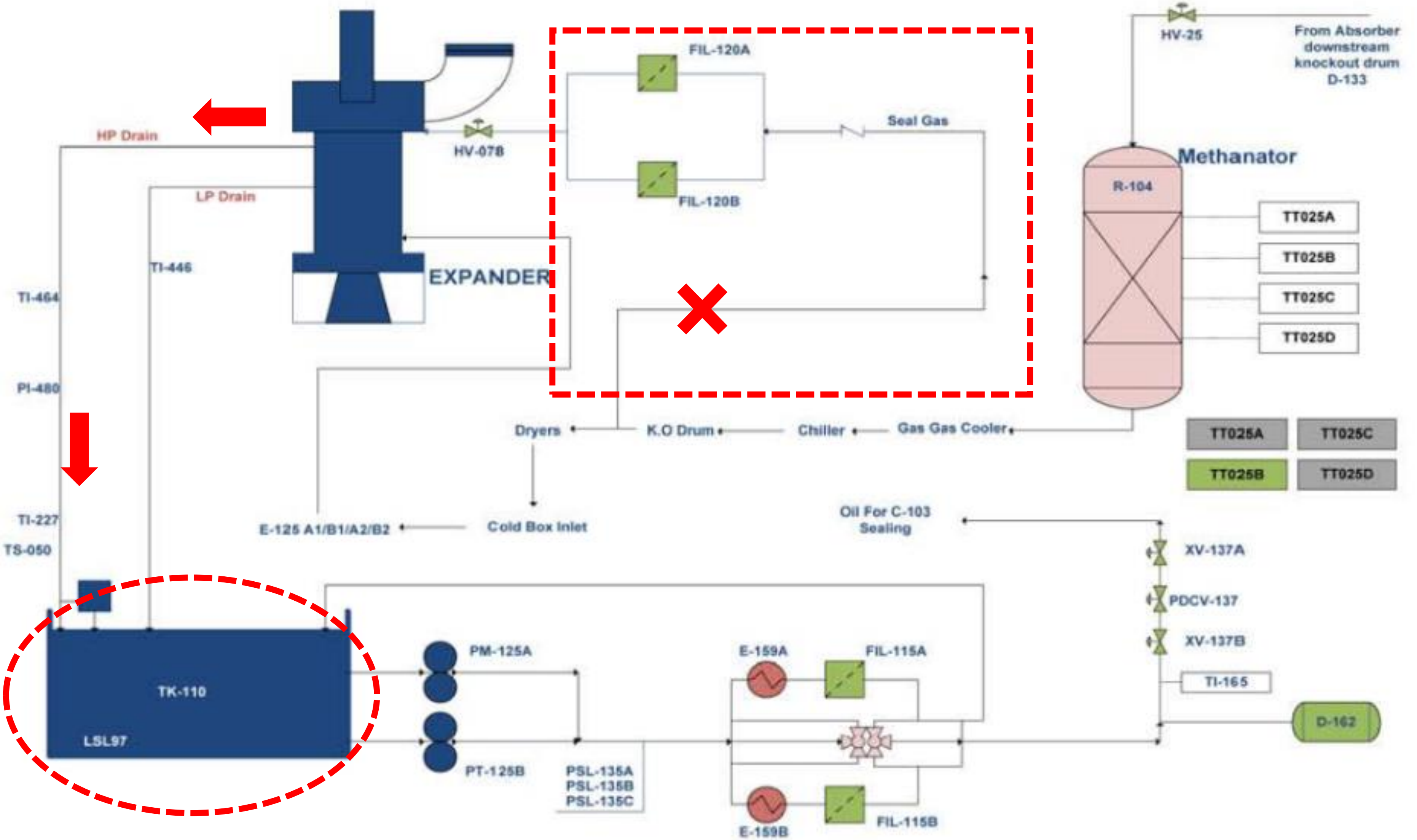
Incident Description

- Foaming in CataCarb solution observed causing excessive and repeated carryover of solution to Methanator.
- Methanator temperature increased to 960°F (515°C) and the Methanator inlet valve HV-25 closed immediately as per control logic.
- However, this also cut the downstream seal gas flow towards the Cold box expander.
- Cold box expander process gas broke through from HP drain to oil console causing console over pressurization and consequently hydrogen fire.

Incident Description



Methanator and Expander



Methanator Selector Switches & Discontinuation of Seal Gas flow caused cold process gas ingress to sour oil return towards oil console

Corrective Actions

1. Control logic modified to automatically trip Cold box expander on:
    - Methanator inlet valve HV-25 closure
    - Differential Pressure across seal gas and HP seal oil < 0.2kg/cm^2
    - Differential Pressure across seal gas and expander casing drops below 0.1 kg/cm^2

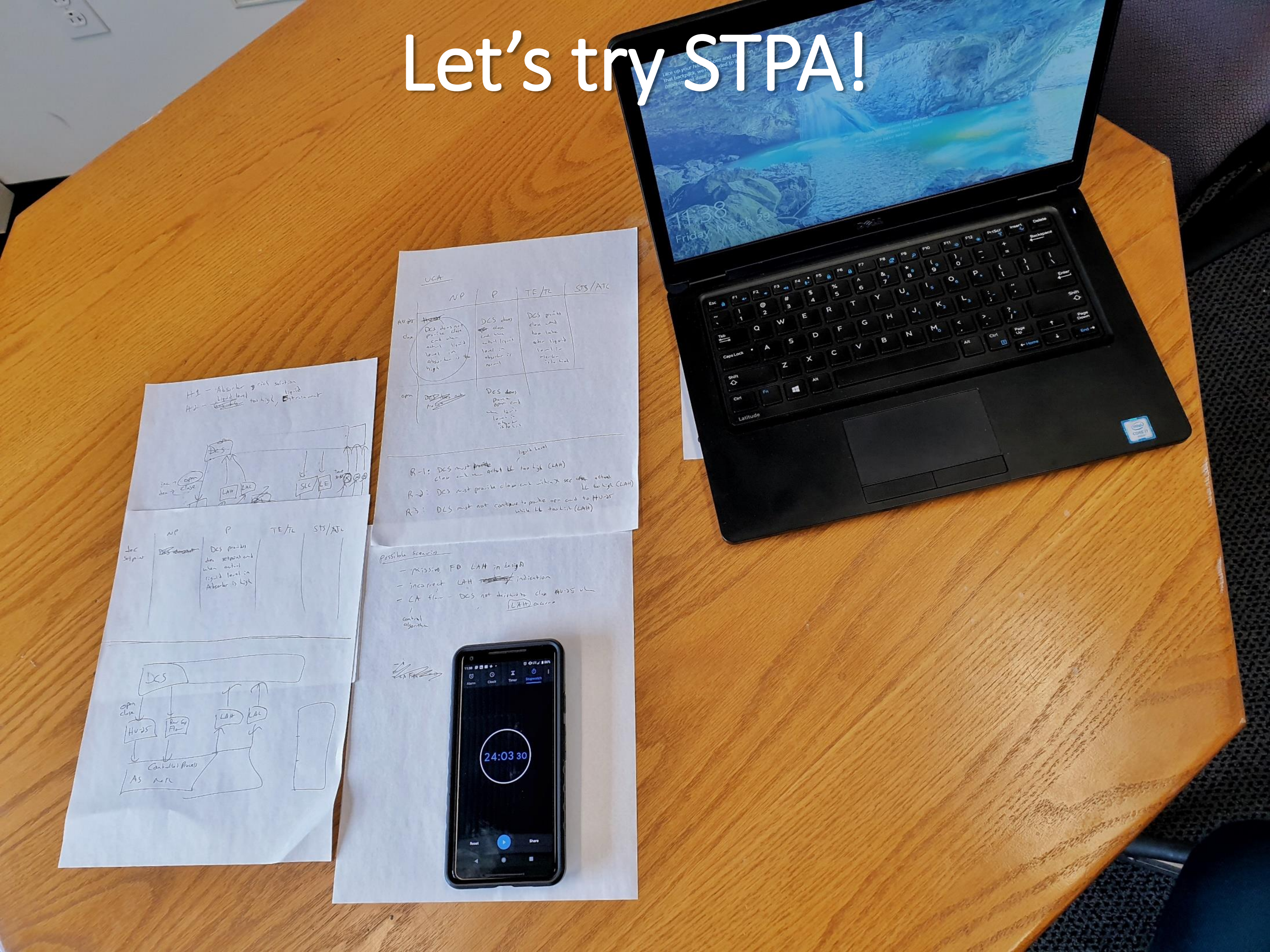
2. Installed a degasifying tank at sour oil HP drain line to avoid oil console over pressurization and consequent fire due to higher seal gas venting.

Safe and smooth plant operation after trip logic and other relevant modifications

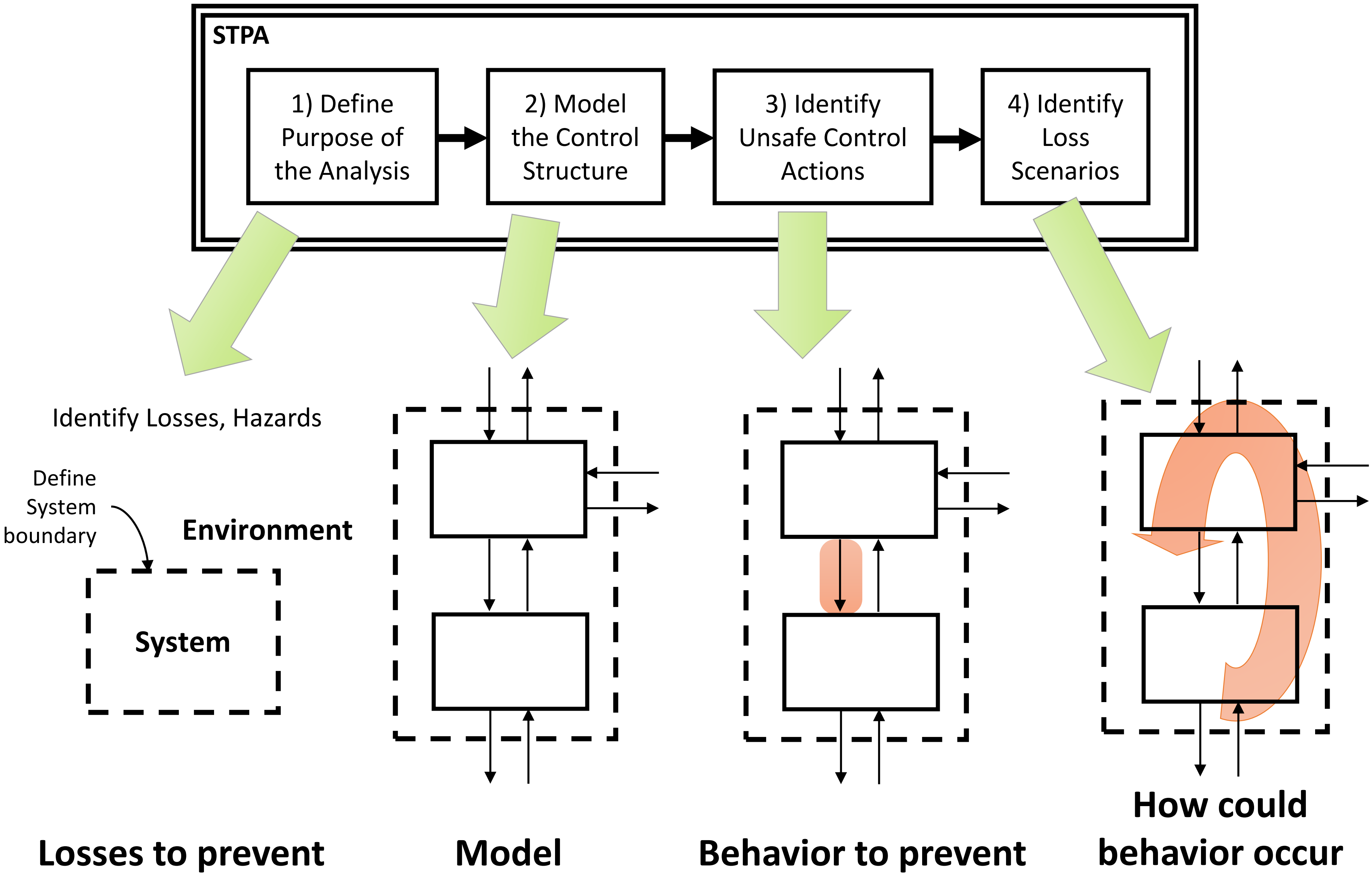
Remarks

- The experienced team did everything as required by the HAZOP methodology, but the requirement was missed.
- Petrochemical/refining processes are complex in nature and there is always a possibility of missing out any critical logic due to nodes/guidewords analyses.

Let’s try STPA!

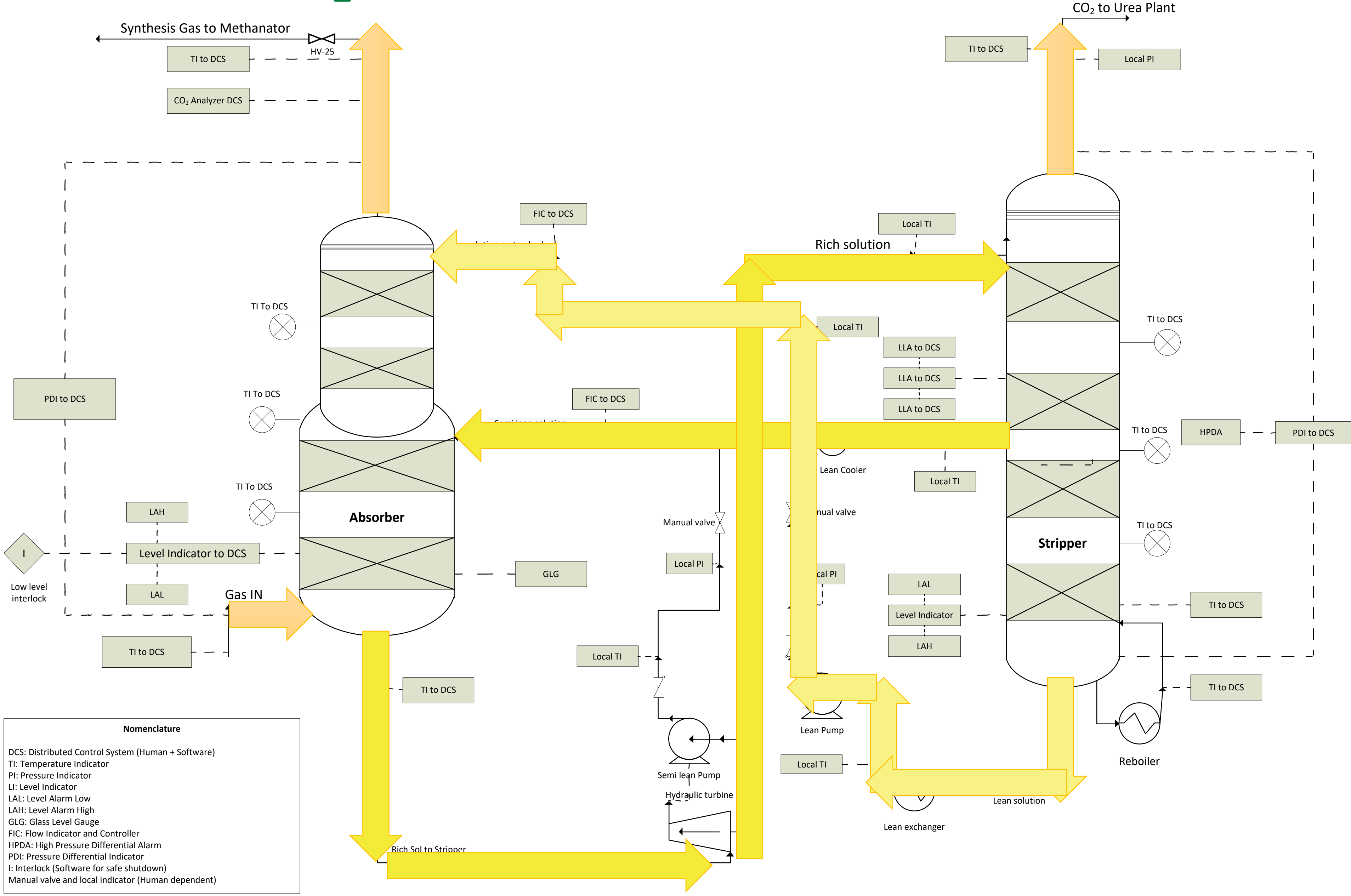


STPA: Hazard Analysis



(Leveson and Thomas, 2018)

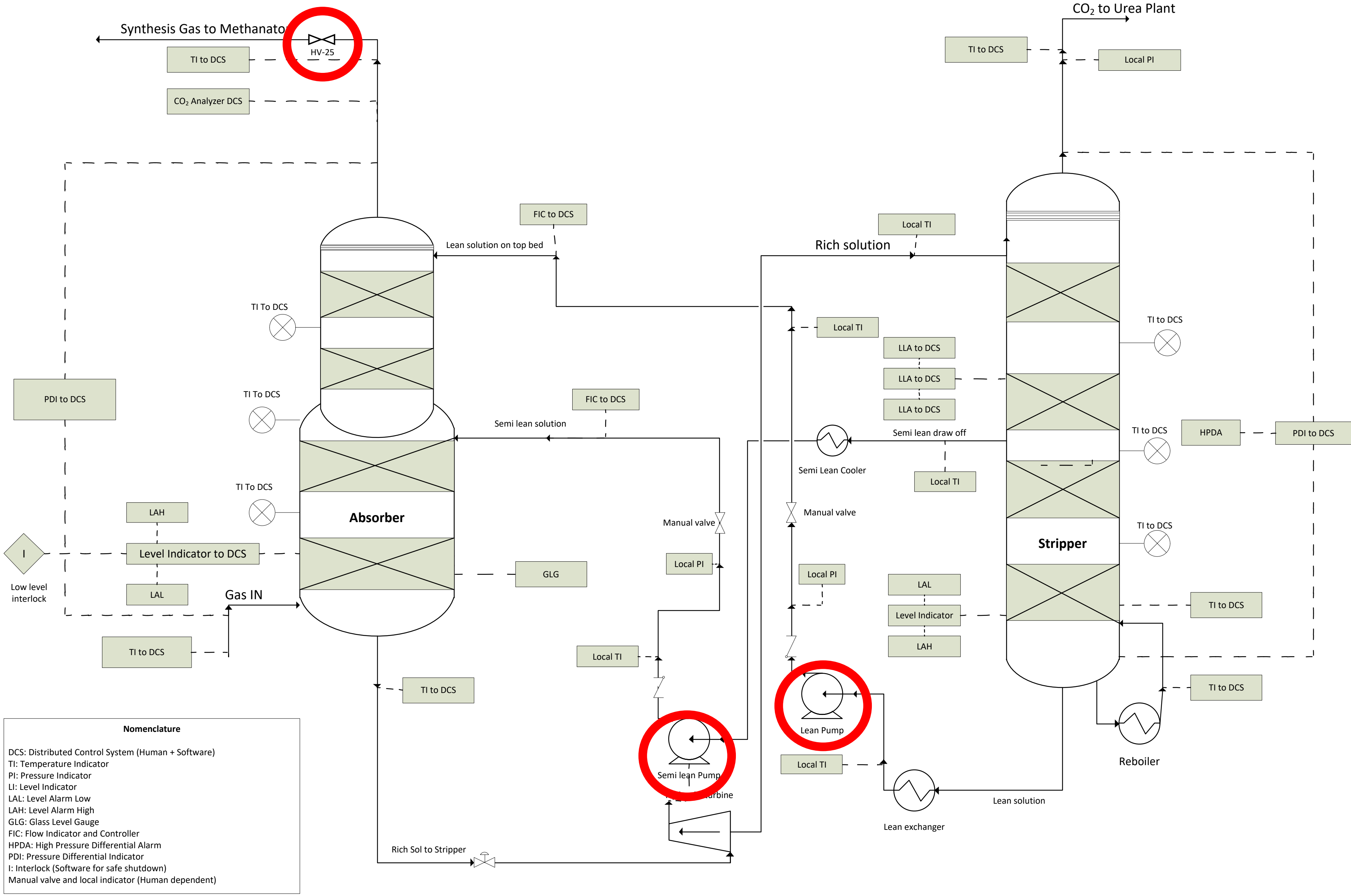
CO_2 Removal System Process Flow



Nomenclature

DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)

DCS/PLC Controls

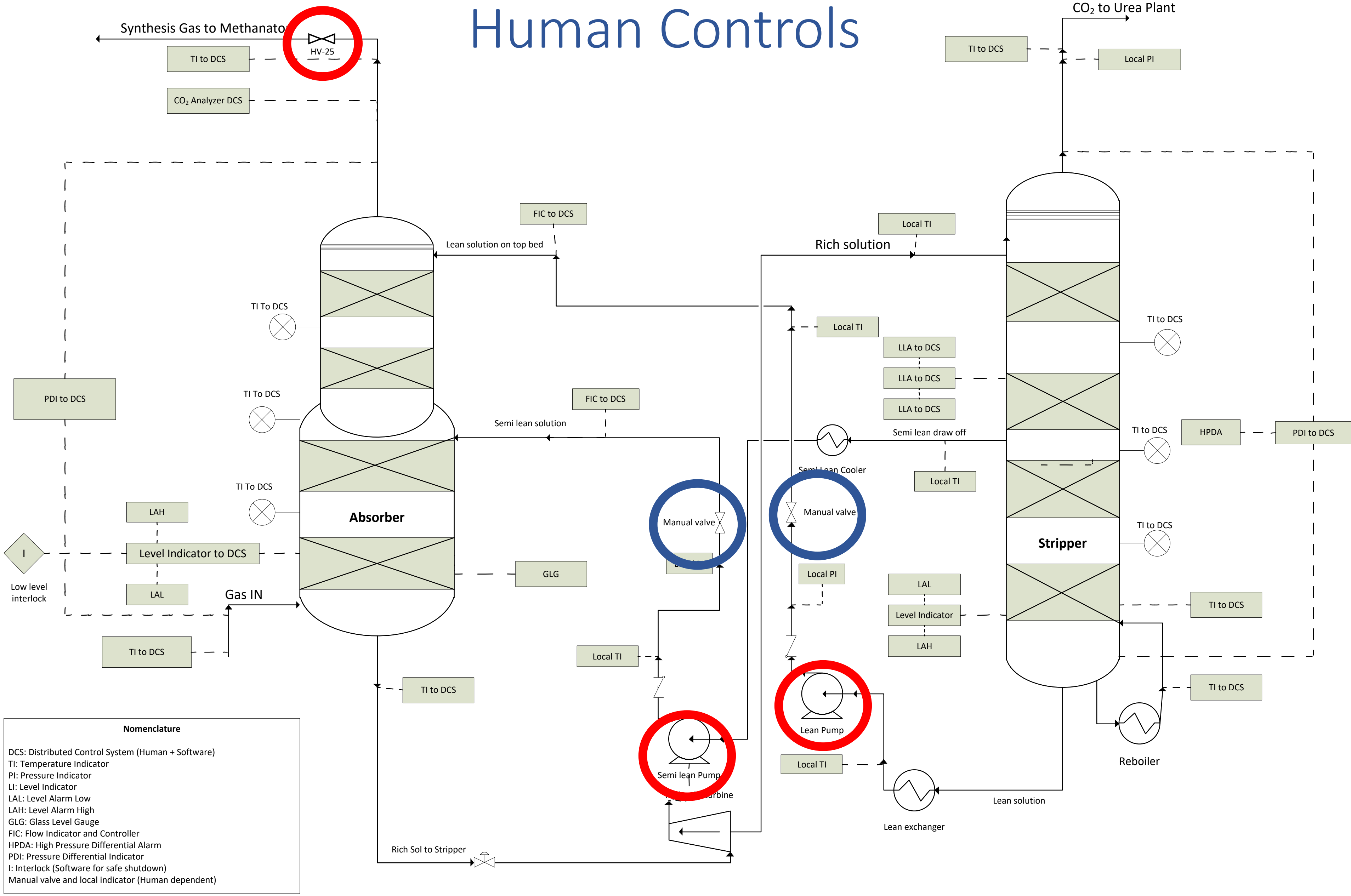


Nomenclature

DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)

DCS/PLC Controls

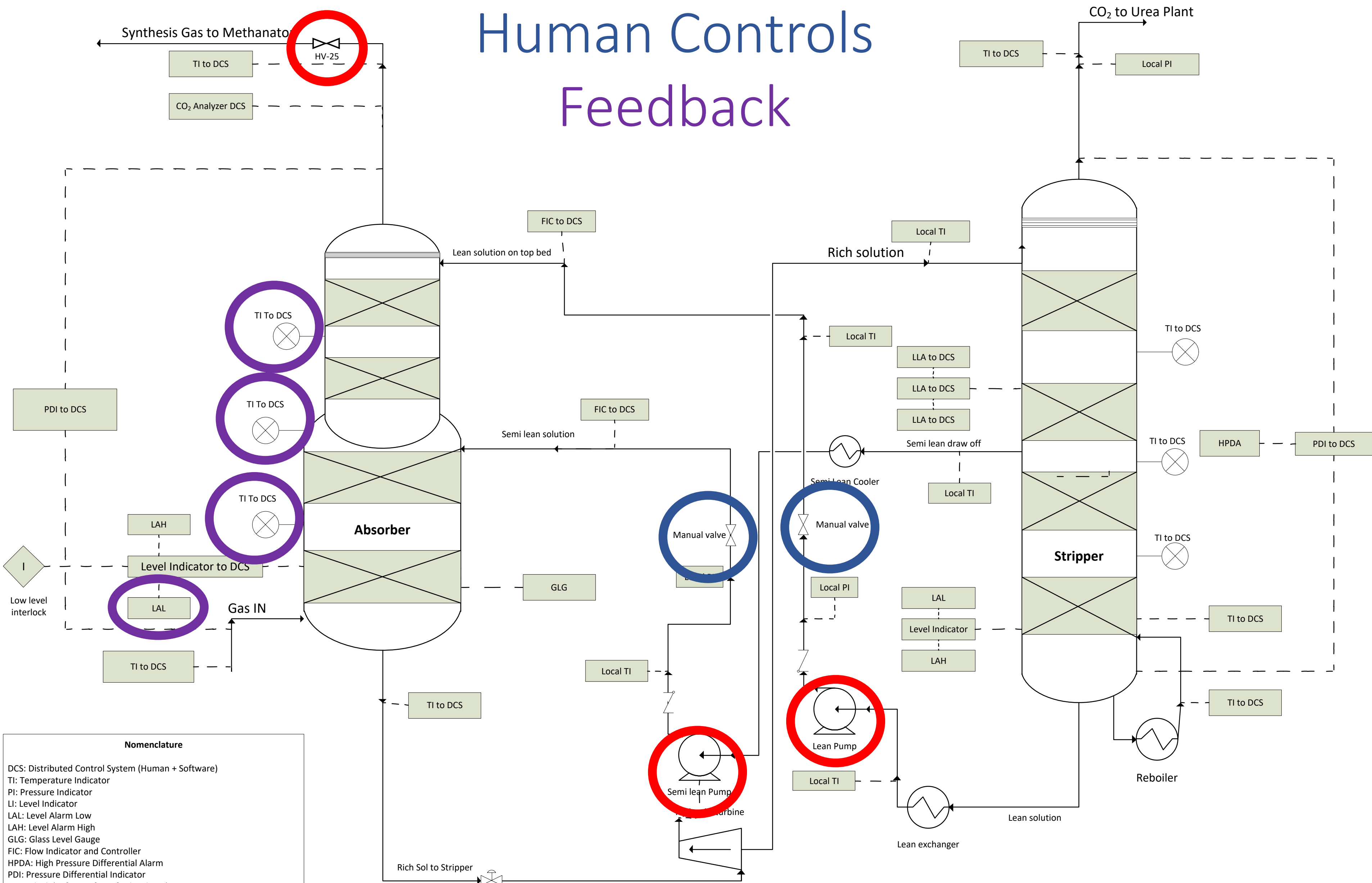
Human Controls



Nomenclature

DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)

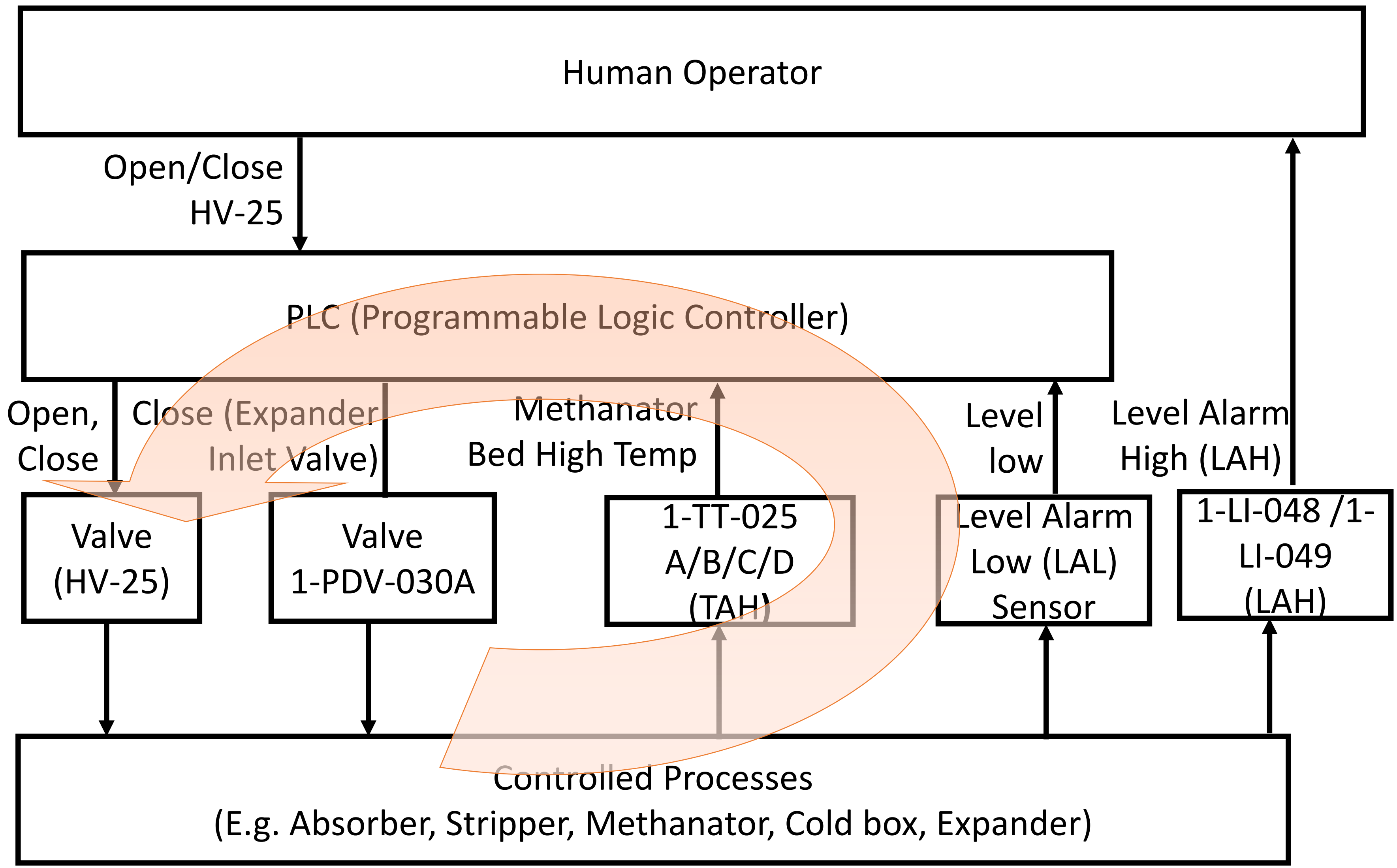
DCS/PLC Controls
Human Controls
Feedback



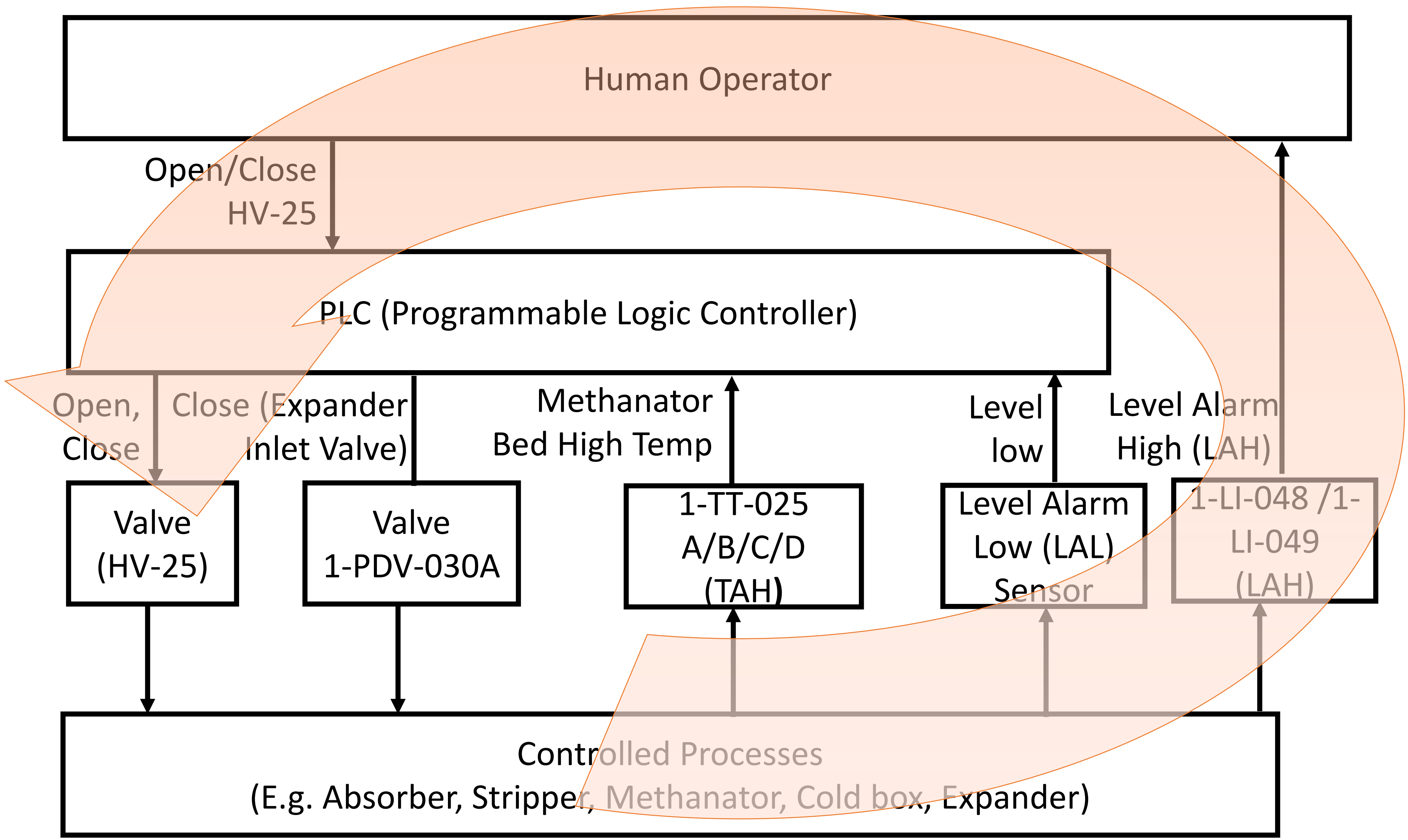
Nomenclature

DCS: Distributed Control System (Human + Software)
TI: Temperature Indicator
PI: Pressure Indicator
LI: Level Indicator
LAL: Level Alarm Low
LAH: Level Alarm High
GLG: Glass Level Gauge
FIC: Flow Indicator and Controller
HPDA: High Pressure Differential Alarm
PDI: Pressure Differential Indicator
I: Interlock (Software for safe shutdown)
Manual valve and local indicator (Human dependent)

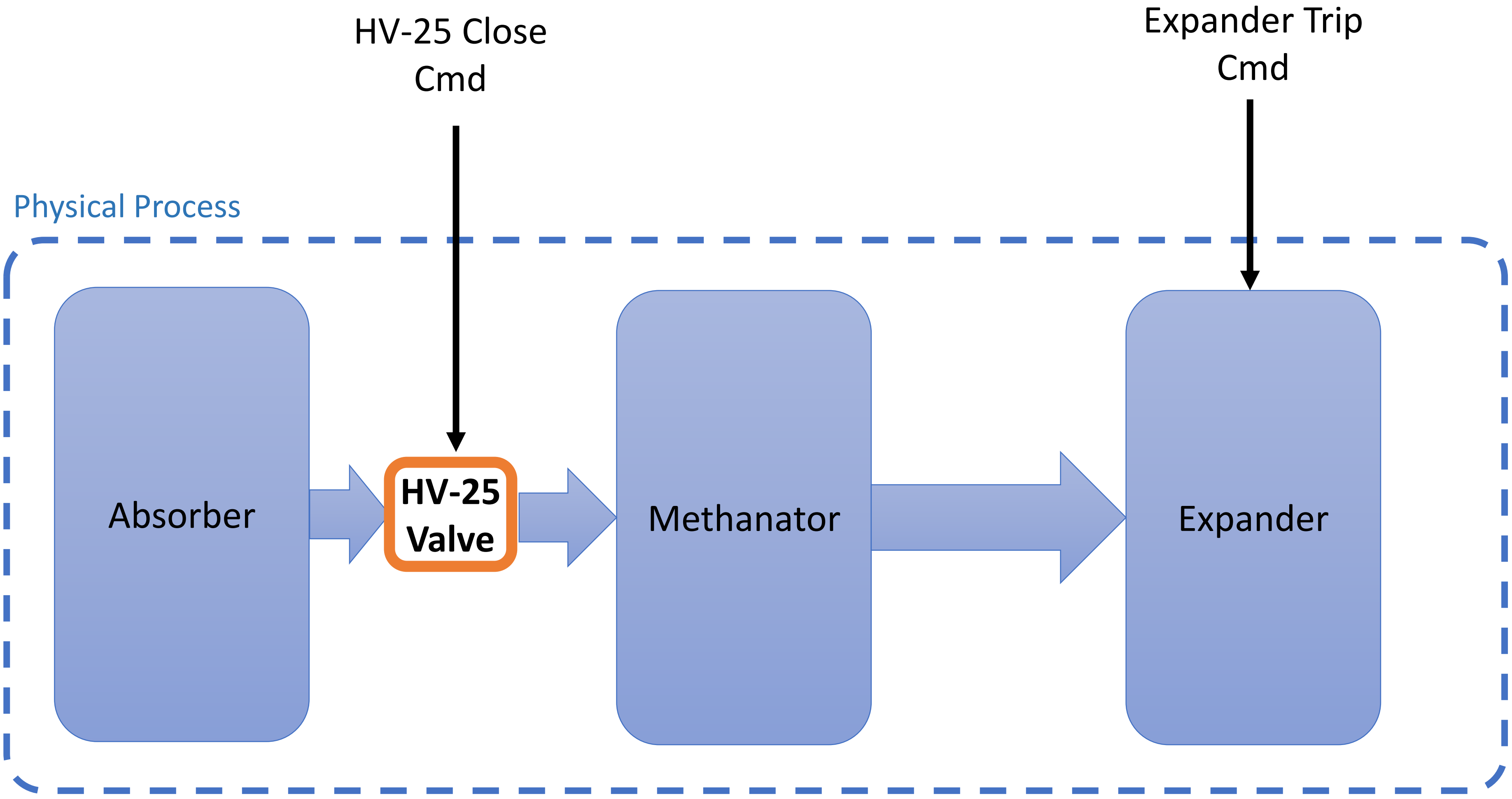
STPA Control Structure Model (Quick sketch)



STPA Control Structure Model (Quick sketch)



A simpler diagram



Fatima
Fertilizer Company Limited

STPA Step 3: PLC Unsafe Control Actions

MIT AEROASTRO

Control Action	Not providing causes hazard	Providing causes hazard	Too early, Too late, Order	Stopped too soon, Applied too long
Close	UCA-1: PLC does not provide Close HV-25 Cmd when actual liquid level is high in the Absorber. [SH-2, SH-3, SH-4]	UCA-2: PLC provides Close HV-25 Cmd when actual liquid level in absorber is normal (cause Methanator trip). [SH-4] **UCA-3: PLC provides Close HV-25 Cmd while expander remains in service (causes low seal gas flow to expander which will eventually result in fire) [SH-1,SH-2,SH-4]**	UCA-4: PLC provides Close HV-25 Cmd too early when liquid level is high (trip set point) [SH-4] UCA 5: PLC provides Close HV-25 Cmd too late when liquid level in absorber is high (causes solution carryover to Methanator causing run away of reaction which will lead to Methanator vessel failure) SH-1,SH-2,SH-4]	UCA-6: PLC continues providing Close HV-25 Cmd too long after liquid level is normal (will prevent startup when issue is resolved) UCA-7: PLC stops providing Close HV-25 Cmd too soon before valve has fully closed UCA-8: PLC stops providing Close HV-25 Cmd too soon before liquid level in absorber has returned to normal
Open	[…]	[…]	[…]	[…]

Fatima

STPA Step 3: Operator Unsafe Control Actions

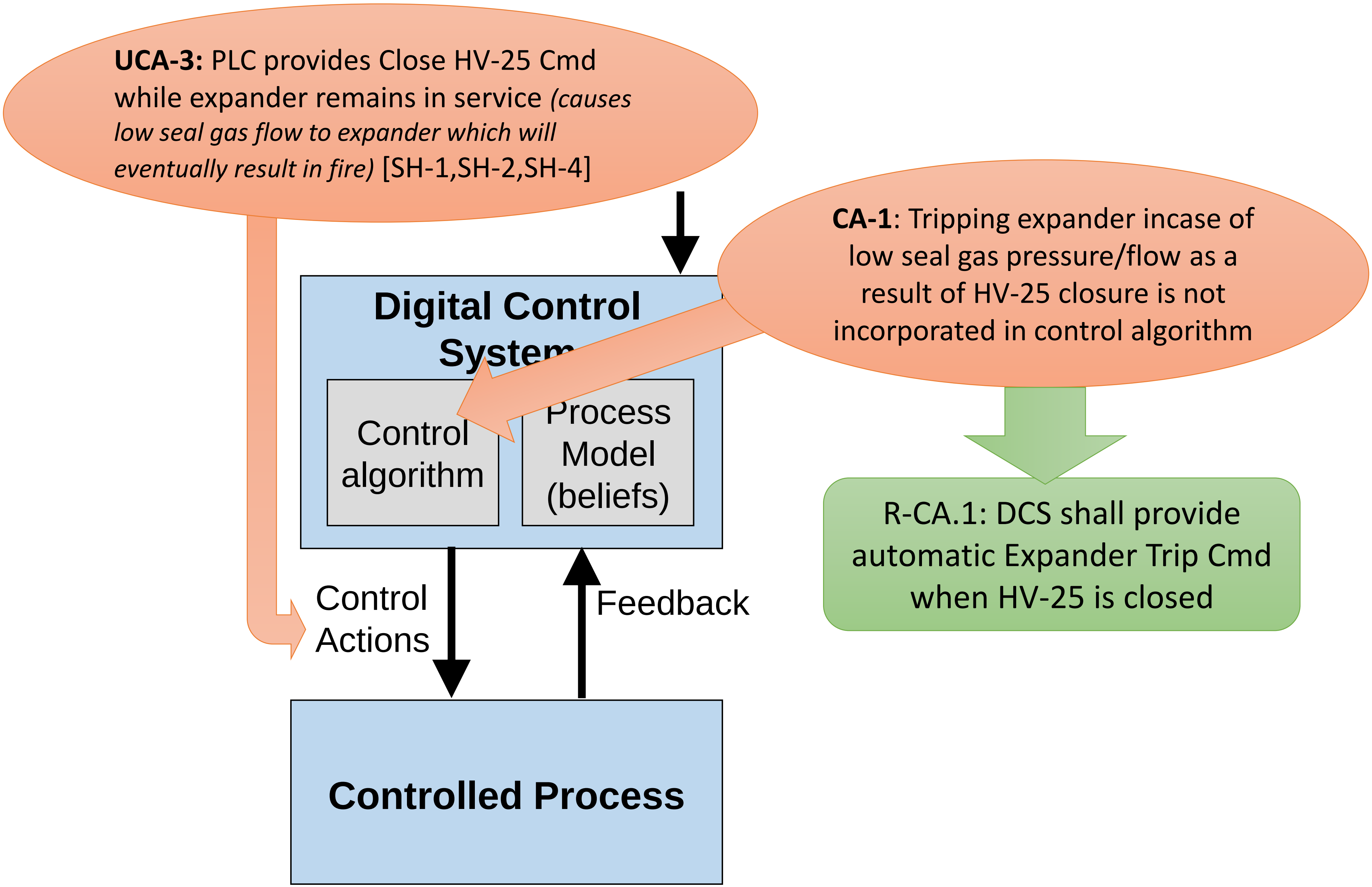
AEROASTRO

Control Action	Not providing causes hazard	Providing causes hazard	Too early, Too late, Order	Stopped too soon, Applied too long
Close	[…]	[…]	[…]	[…]
Open	UCA-17: Operator does not provide Open HV-25 Cmd during startup [SH-3, SH-4]	UCA-18: Operator provides Open HV-25 Cmd when liquid level is high [SH-2, SH-4]	UCA 19: Operator provides Open HV-25 Cmd too soon during startup (causes quick pressurization of Methanator will result in leakage, catalyst damage, etc.) [SH-1, SH-2, SH-3, SH-4] UCA 20: Operator provides Open HV-25 too late during startup [SH-2, SH-4]	UCA-21: Operator continues providing Open HV-25 Cmd too long when liquid level is high [SH-2, SH-4] UCA 22: Operator provide Open HV-25 Cmd too soon during startup which cause high CO_2 slippage enter Methanator and will cause temperature run away. [SH-1, SH-2, SH-3, SH-4]

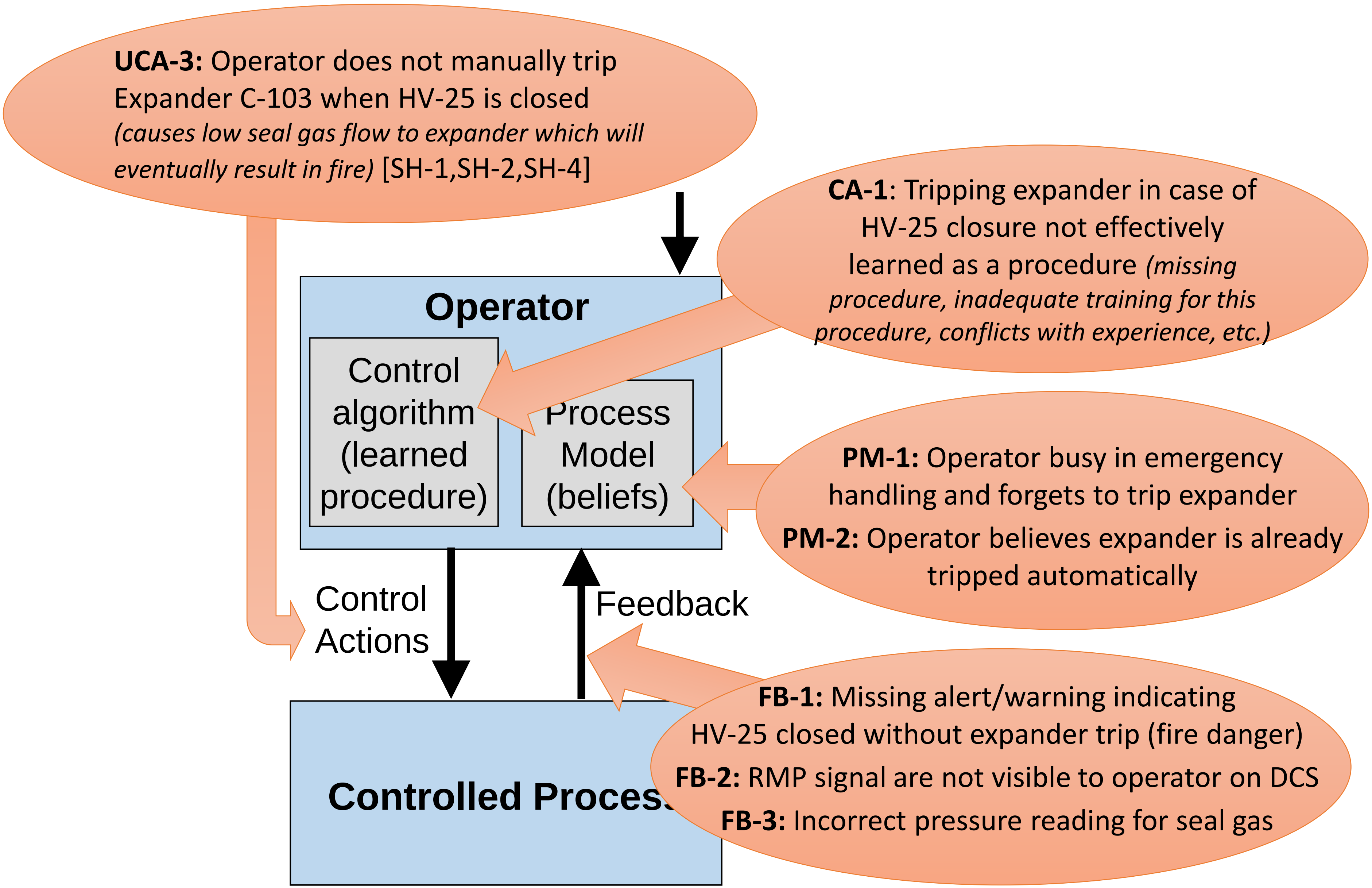
Generating DCS Functional Requirements

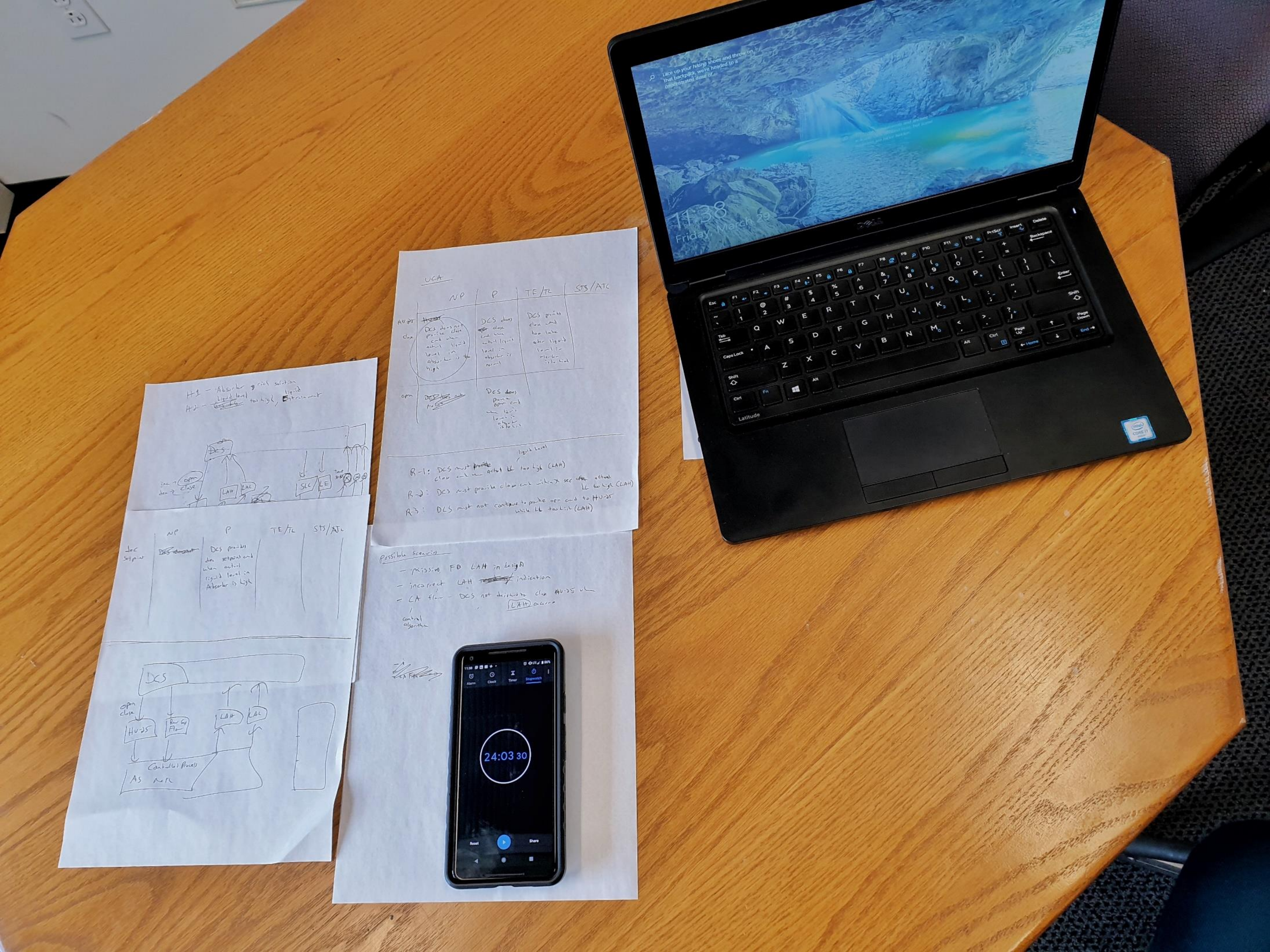
Unsafe Control Action	Controller Requirement
UCA-1: DCS does not provide Close MV-25 cmd when actual liquid level in absorber is too high	R-UCA1: DCS shall provide Close MV-25 cmd when actual liquid level in absorber is too high (LAH=true) [**UCA-1**]
UCA-3: DCS provides Close MV-25 cmd too late (>10 sec) after liquid level in absorber is too high	R-UCA3: DCS shall provide Close MV-25 cmd within <10 sec of liquid level in absorber too high [**UCA-3**]
UCA-6: DCS provides Open MV-25 cmd when liquid level in absorber is too high	R-UCA6: DCS must not provide Open MV-25 cmd while liquid level in absorber is too high [**UCA-6]**

STPA Step 4: Building Accident Scenarios



STPA Step 4: Building Accident Scenarios





Conclusion

At the time of detailed engineering of Catacarb unit, **the potential Hazard was not anticipated** against the HAZOP guide word of **no flow** to expander. Similarly **the consequence was not captured during HAZOP** under Methanator upstream valve closure **due to two separate nodes**.

Therefore, it may be concluded that this specific and well recognized technique “HAZOP” may be limiting in capturing all the hazards even if applied as per defined methodology/guideline.

However, STPA did result in identifying the missing control logic.

Thank You