Model Checking of the Process Control Program for a Hydrogen Pilot Plant

Burak ÖKTEN

Halit OĞUZTÜZÜN

METU, Ankara

IZTECH 4th Workshop on Dependability

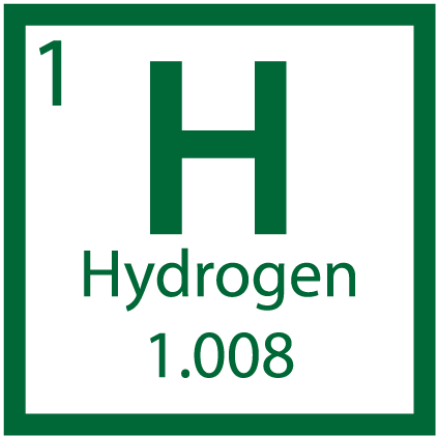
21 May 2018

• OUTLINE

1. Introduction
2. Problem Statement
3. About Pilot Plant
4. System Model
5. Analysis
6. Conclusion & Future Work
7. References

• INTRODUCTION (1/4)

- Hydrogen is a strong fuel candidate of future. It has many usage areas as a chemical reagent and as a rocket propellant.
- Today, one of the research areas of hydrogen usage is transportation.
- There are two common methods take place to produce hydrogen [1]:
  1. Reforming / gasification of hydrocarbons such as methane (CH4) and methanol (CH3OH).
  2. Electrolysis of water (H2O).



• INTRODUCTION (2/4)

Why is hydrogen production safety critical?

1. Hydrogen is lighter than air and it has a very high diffusivity (20 m/s).
2. Hydrogen is odorless, colorless and tasteless.
3. Hydrogen can combust.
4. Hydrogen can cause explosions, if at least 10% oxygen is present.
5. Hydrogen can cause freeze burns when it is in liquid state at low pressure (-252.87°C and 1.013 bar) [2, 3].

• INTRODUCTION (3/4)

What can happen in a chemical plant if precautions are not enough to operate processes safely?

In 2005, an explosion at the BP Texas City Refinery caused 15 dead, 170 injured and over $2 billion total cost!

Main reason:

Overpressure in the blowdown drum due to overfilling of the distillation tower.

Why happened?

- Liquid level detection system was inaccurate.
- Ignoring the abnormal behaviour of control valves, alarms and level detectors.
- Lack of attention on system operation [4].

• INTRODUCTION (4/4)

Figure 1. The explosion was catastrophic. *

* Retrieved from https://www.csb.gov/statement-of-chairperson-vanessa-allen-sutherland-on-the-12th-anniversary-of-the-bp-texas-city-refinery-disaster/

• PROBLEM STATEMENT

- Hydrogen production consists of a series of safety critical processes. Predicting extreme problematic states of these operations using simulations is difficult. Thus, model checking approaches should be evaluated [5].

- In this project, following cases were studied for APS Hydrogen Fuel Pilot Plant:
    1. Performing model checking to verify the safety features of the process control system using **Promela** and **iSpin.**
    2. Finding of possible process failures using the verification of the plant control logic.

• ABOUT PILOT PLANT (1/3)

Figure 2. APS Hydrogen Pilot Plant, Phoenix, Arizona [1].

• ABOUT PILOT PLANT (2/3)

Highlights:

1. Hydrogen is produced from high-purity water using electrolysis (18 kg / day).
2. Dryer removes water from hydrogen to reach 99.9999% purity.
3. Low pressure tank stores hydrogen (up to 20 kg) in 150 psig.
4. It is compressed to 5800 psi and stored (up to 20 kg each) in high-pressure tanks.
5. Hydrogen is transported to a tube trailer with a dispenser unit.
6. The system is monitored with proper sensors.
7. The plant is continuously scanned for infrared and ultraviolet radiation (signatures of a hydrogen flame).
8. Gas detectors are also used to monitor for flammable gases.
9. The EMS enables complete system shutdown automatically or manually [1].

• ABOUT PILOT PLANT (3/3)

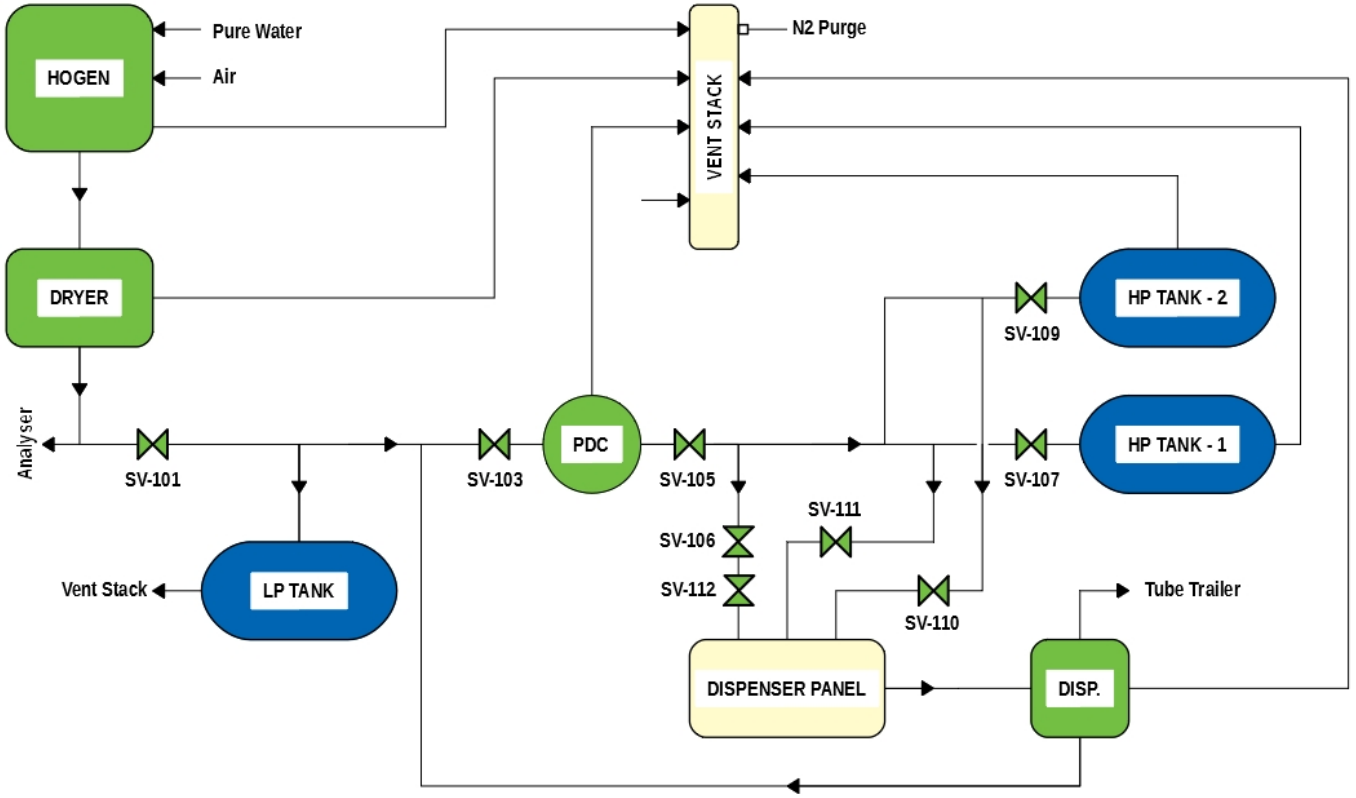


Figure 3. Process flowchart for the plant.

• SYSTEM MODEL (1/7)

Following steps were performed to obtain system model:

1. Determining of the plant processes.
   - Hydrogen production.
   - Water removal from hydrogen (drying).
   - Compressing.
   - Storing.
   - Dispensing.
   - Venting.
2. Simplifying of these processes using plant P&ID.
   - Avoid adding unnecessary details. It causes increase of the state space and generally result doesn't change [5].
3. Preparing of relations and rules between operations and equipment.
4. Designing of system model.

• SYSTEM MODEL (2/7)

- Promela language and iSpin tool were used to develop SPIN model of **process control program** and **all plant operations.**
- Event → Sensor → Controller → Equipment

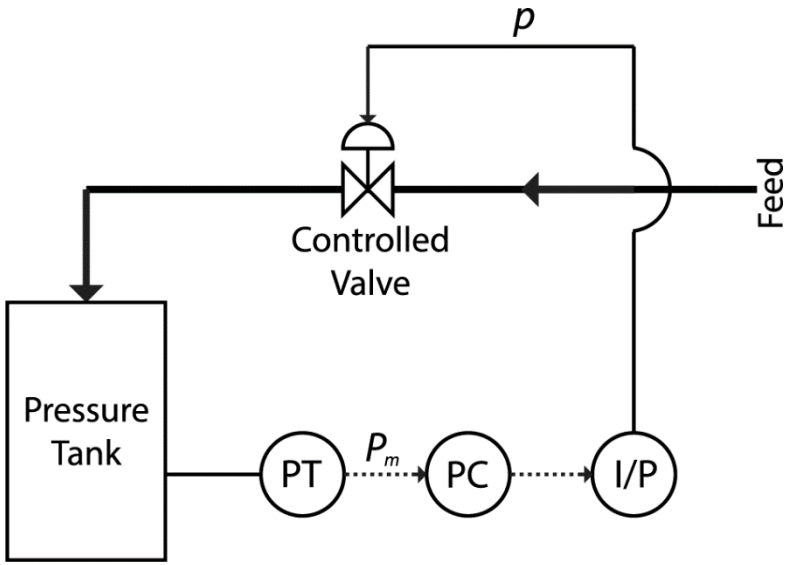


Figure 4. An example of a pressure control system.

• SYSTEM MODEL (3/7)

- Rendezvous signals were used from sensors to controller and from controller to equipment.
- Assumptions:
  - The control program will work independently of the time (untimed model).
  - Safety related valves only.

• SYSTEM MODEL (4/7)

Modelled equipment:

- 4 main units (Hogen, Dryer, PDC Compressor, and Dispenser).
- 10 safety valves.
- 13 sensors (UV/IR, CGD, LDS and pressure sensors).
- 1 Emergency Shutdown System.
- 1 main controller.
- 1 alarm and 1 callout systems.

• SYSTEM MODEL (5/7)

```
proctype SV105() {
    bool msg;
    do
    :: ch_105_from ? msg ->
                if
                :: SV_105_ON ->
                        atomic {
                            SV_105_ON = false;
                            SV_105_H2 = false;
                            printf("SV105 IS OFF \n")
                        };
                        SV_106_H2 = false;
                        SV_107_H2 = false;
                        SV_109_H2 = false;
                        SV_110_H2 = false;
                        SV_111_H2 = false;
                        SV_112_H2 = false
                :: SV_105_ON ->
                        atomic {
                            sv105_fail = true;
                            printf("SV105 FAILED TO CLOSE \n")
                        }
                :: else -> skip
                fi
    od
}
```

Figure 5. Promela model of SV-105 valve.

• SYSTEM MODEL (5/7)

```
proctype PT110_SENSOR() {
    do
    :: Disp_H2_P == _HIGH_ ->
            atomic {
                printf("PT110 DETECTED HIGH P ON DISPENSER H2 P \n");
                ch_pt_110_to ! true;
                ch_alarm_to ! _P1_
            }
    :: Disp_H2_P == _VHIGH_ ->
            atomic {
                printf("PT110 DETECTED VHIGH P ON DISPENSER H2 P \n");
                ch_pt_110_to ! true;
                ch_alarm_to ! _S1_
            }
    od
}
```

```
proctype ControlPanel() {
    bool msg;
    mtype mtp;
    do

    ...

    :: ch_pt_110_to ? msg ->
            atomic {
                printf("CONTROLLER RECEIVED A SIGNAL FROM PT110 \n");
                ch_106_from ! false;
                ch_110_from ! false;
                ch_111_from ! false;
                ch_112_from ! false
            }
    ...

    od
}
```

Figure 6. Promela models of PT-110 sensor and its controller.

• SYSTEM MODEL (6/7)

Modelled events and states:

- LP Tank pressure level change.
- PDC Compressor leakage state.
- PDC Compressor outlet pressure level change.
- PDC Compressor to HPS pipeline pressure level change.
- PDC Compressor to vent stack state.
- HP Tank-1 and -2 pressure levels change.
- Dispenser pressure level change.
- HPS high flow state.
- Water removal state of Dryer.

• SYSTEM MODEL (7/7)

```
proctype HPTank1() {
    do
    :: SV_107_H2 ->
            if
            :: HP_Tank_1_P == _NOR_ ->
                    atomic {
                        HP_Tank_1_P = _NOR_;
                        printf("HP TANK 1 P IS NORMAL \n")
                    }
            :: HP_Tank_1_P == _NOR_ ->
                    atomic {
                        HP_Tank_1_P = _HIGH_;
                        printf("HP TANK 1 P IS HIGH \n")
                    }
            :: (HP_Tank_1_P == _NOR_ || HP_Tank_1_P == _HIGH_) ->
                    atomic {
                        HP_Tank_1_P = _VHIGH_;
                        printf("HP TANK 1 P IS VERY HIGH \n")
                    };
                    goto exit
            fi
    :: !SV_107_H2 -> goto exit
    od;
    exit: skip
}
```

Figure 7. Promela model of HP Tank-1 pressure levels.

• ANALYSIS (1/6)

- Safety critical conditions of the system model must be verified via model checking.
- Use LTL (Linear Temporal Logic) to claim safety properties.

What is the minimum points of failure count?

- Minimum points of failure count ↓ Process safety ↓
- Independence between failures ↑ Process safety ↑

Critical states with lesser points of failure and maximum dependence must be found.

• ANALYSIS (2/6)

Hydrogen Leakage on PDC Compressor

PDC Compressors are normally robust to leakage. However, water contamination in hydrogen can cause damage and leakage in compressor [1].

Is hydrogen leakage a possible state for this system?

- Dryer is open → water removal.
- What if there is a leak in compressor while Dryer is open?
- How to find this safety critical state?

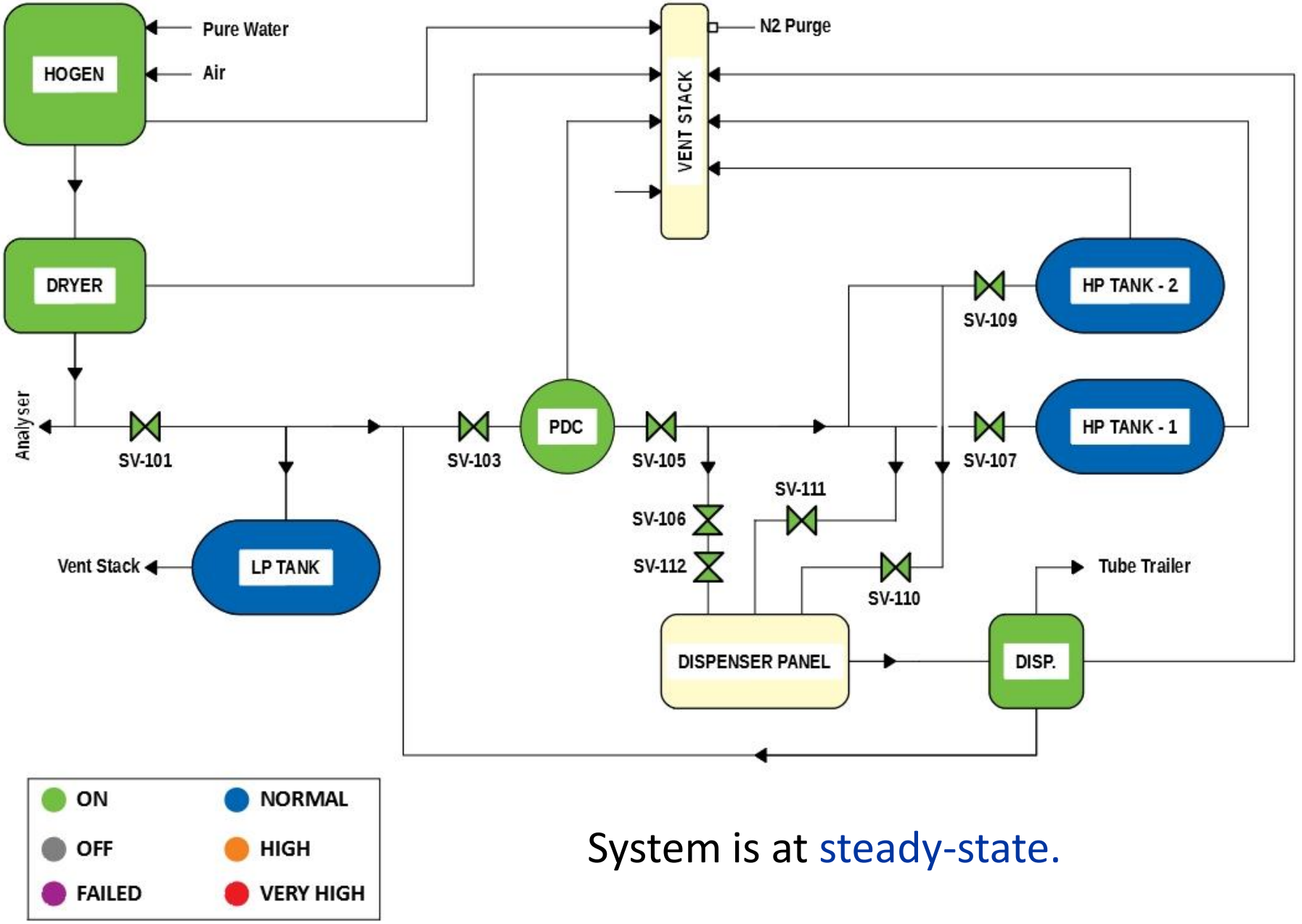
• ANALYSIS (3/6)

Is there a state with PDC Compressor leakage while

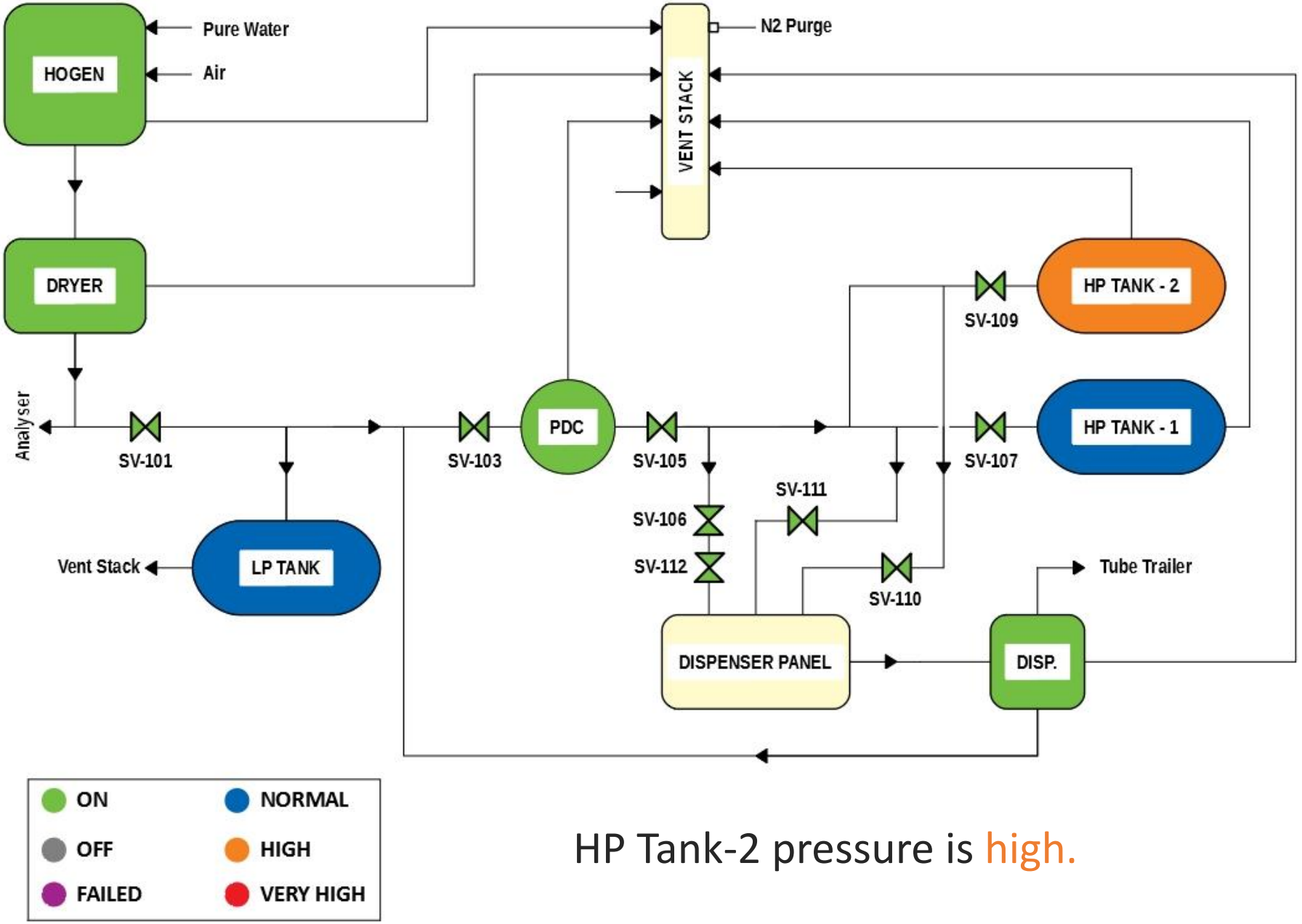
1. Hogen, Dryer and PDC Compressor are open.
2. No Hogen and PDC Compressor fail.
3. Water contamination in hydrogen exists.
4. No valve fail except SV-101 (outlet valve of Dryer) ?

Claim “p1” must be result with a counterexample:

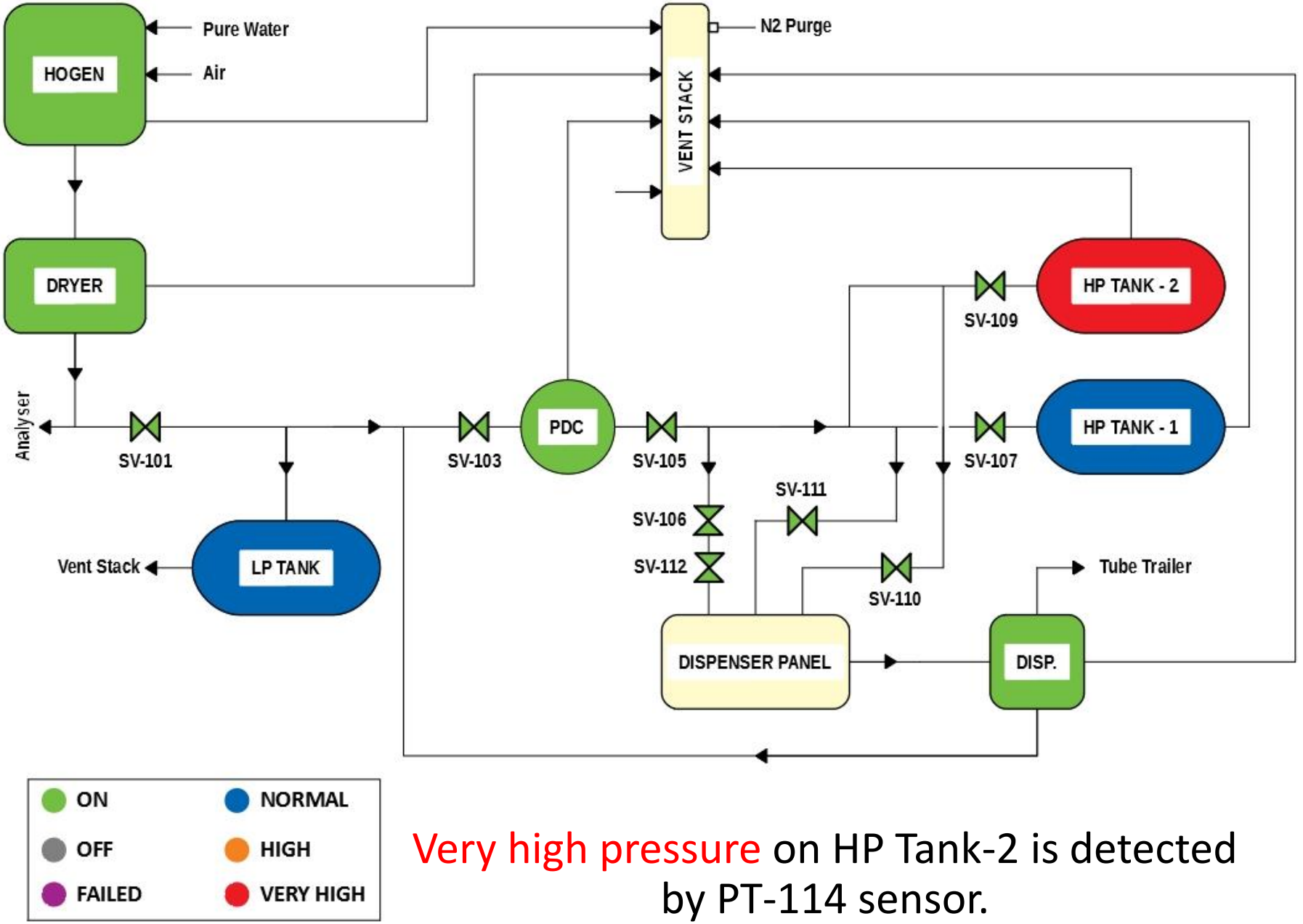
```
ltl p1 {
    [](PDC_Leak -> (!Dryer_ON || !Hogen_ON ||
           !PDC_ON || hogen_fail || pdc_fail ||
           !wet_hydrogen || !sv101_fail ||
           sv103_fail || sv104_fail || sv105_fail ||
           sv106_fail || sv107_fail || sv109_fail ||
           sv110_fail || sv111_fail || sv112_fail))
}
```



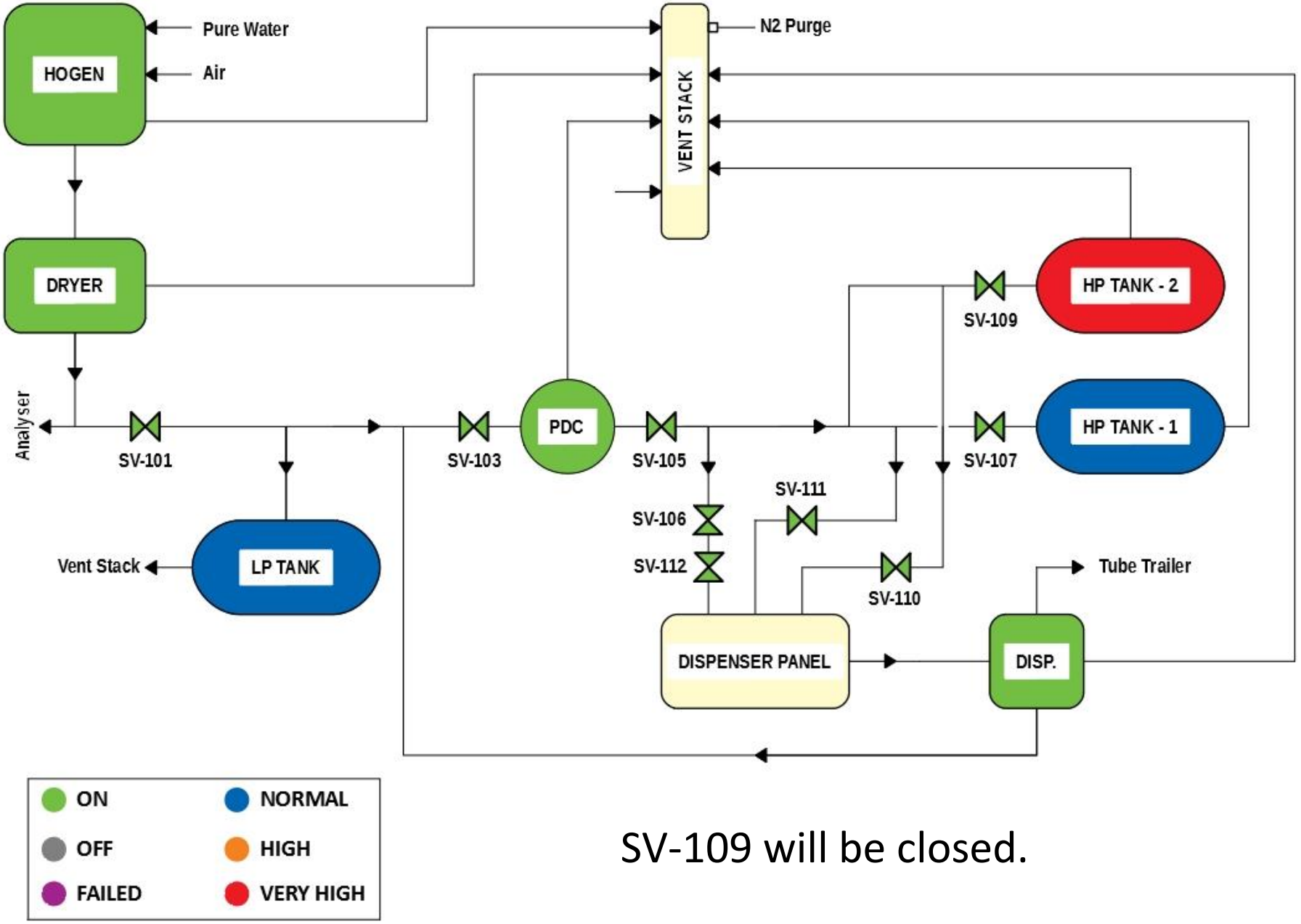
System is at steady-state.



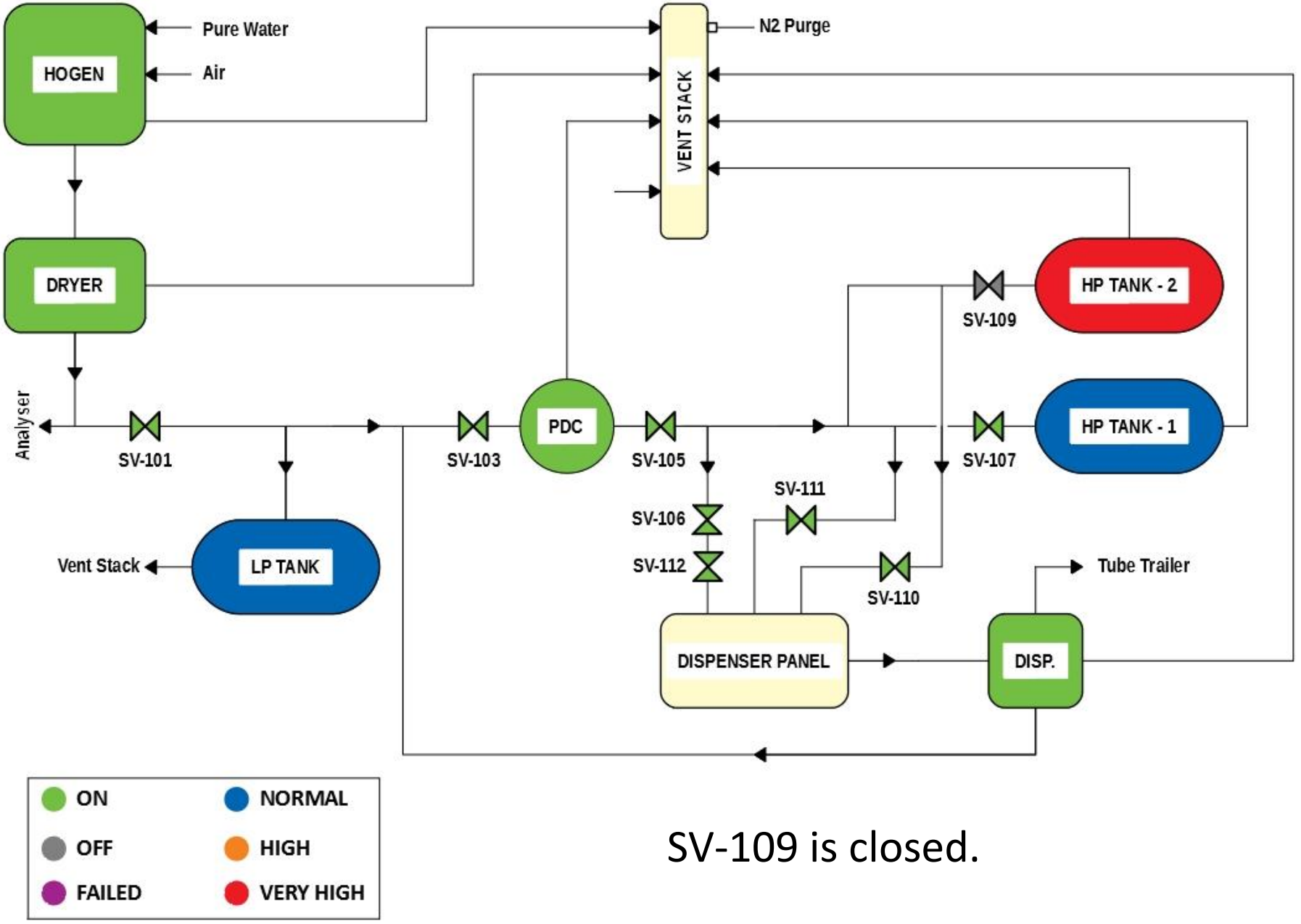
HP Tank-2 pressure is high.



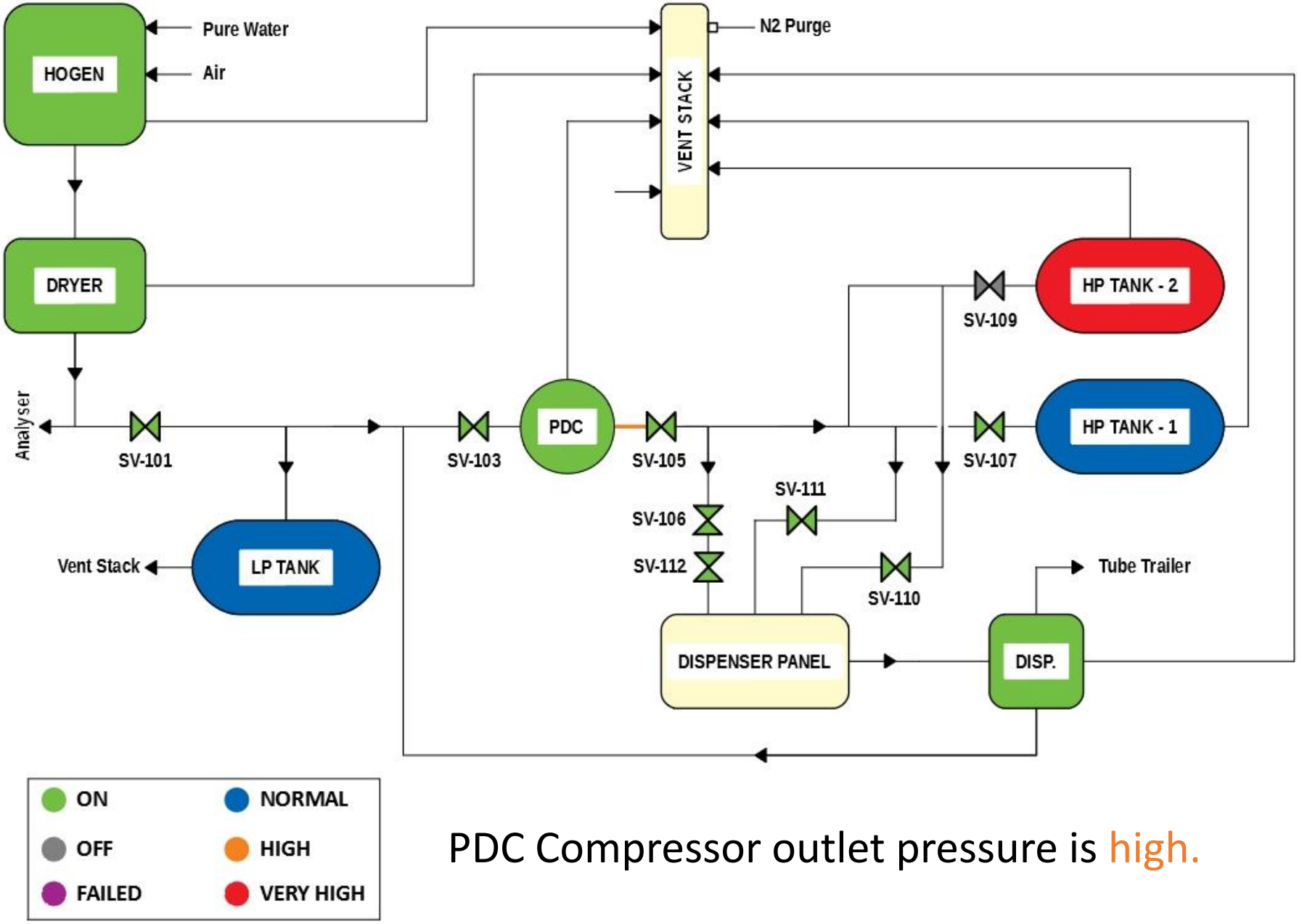
Very high pressure on HP Tank-2 is detected by PT-114 sensor.



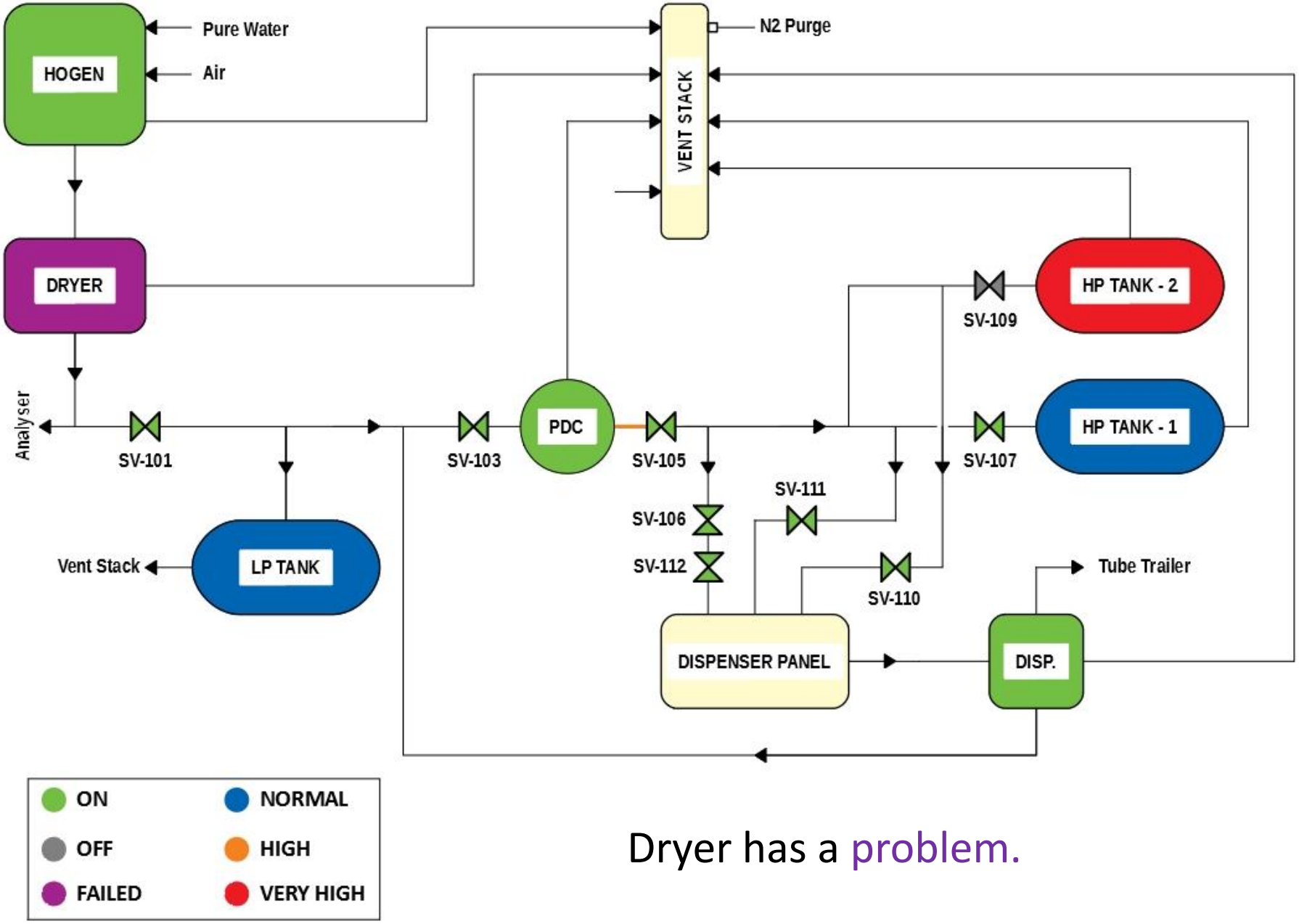
SV-109 will be closed.



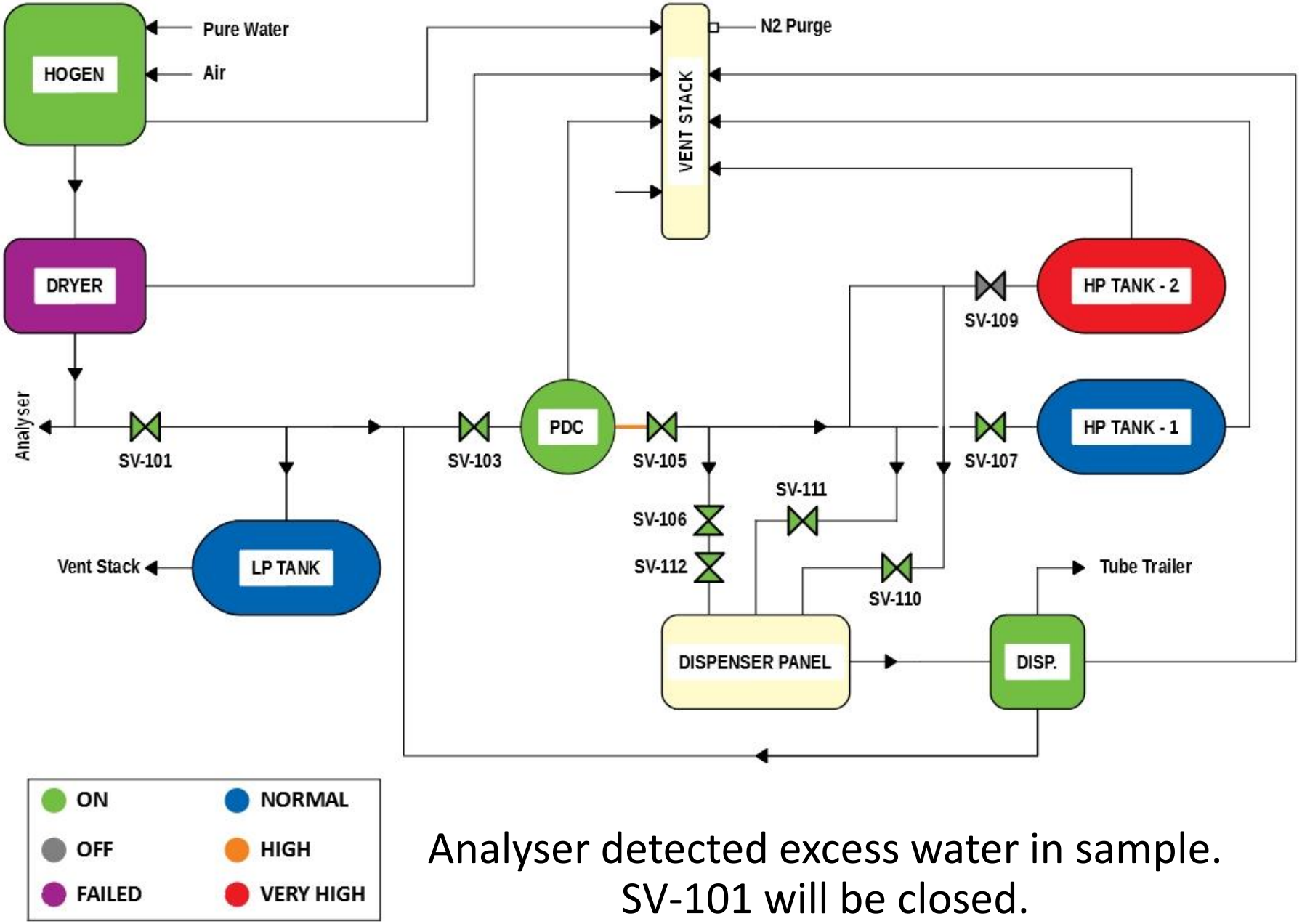
SV-109 is closed.



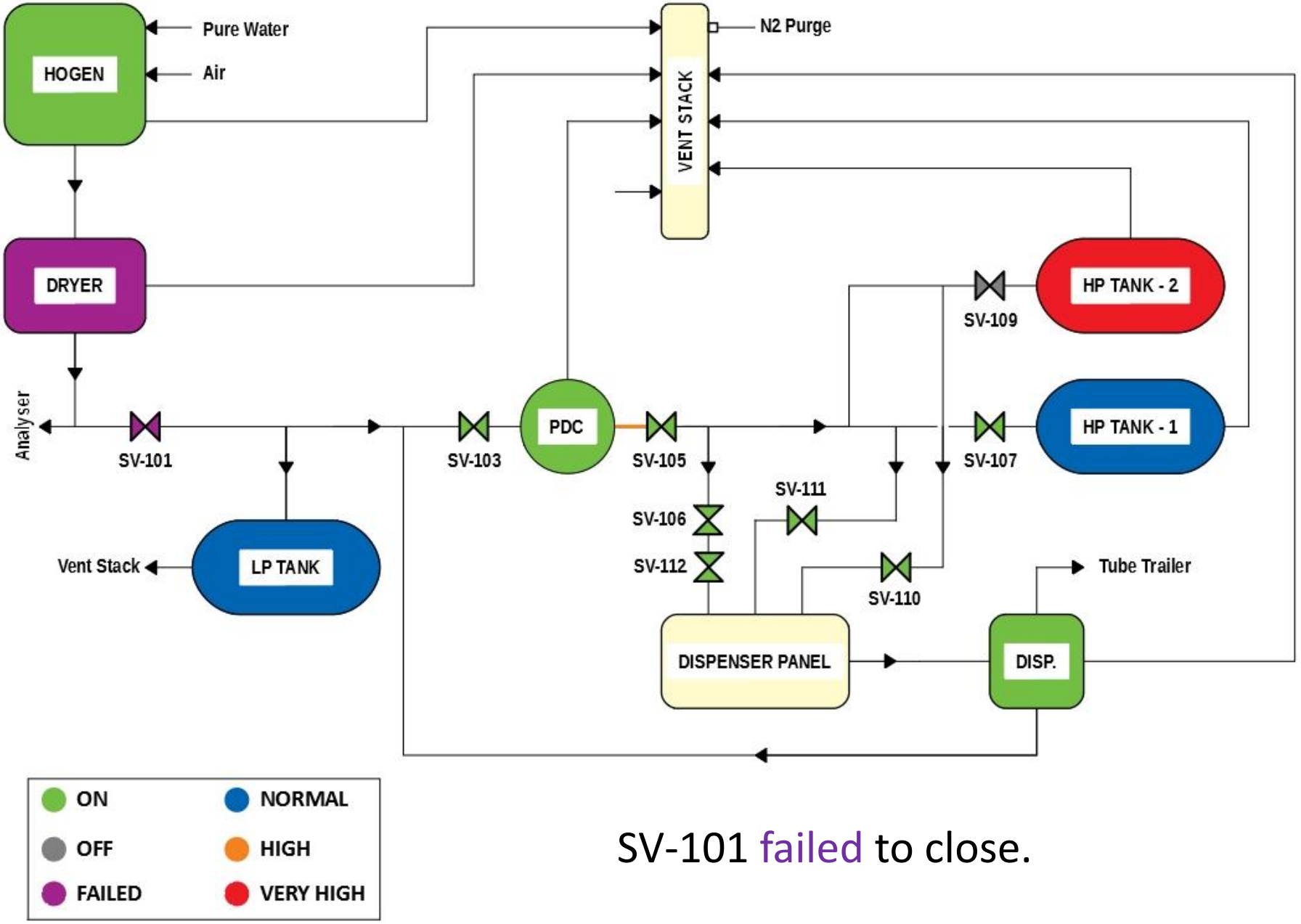
PDC Compressor outlet pressure is high.



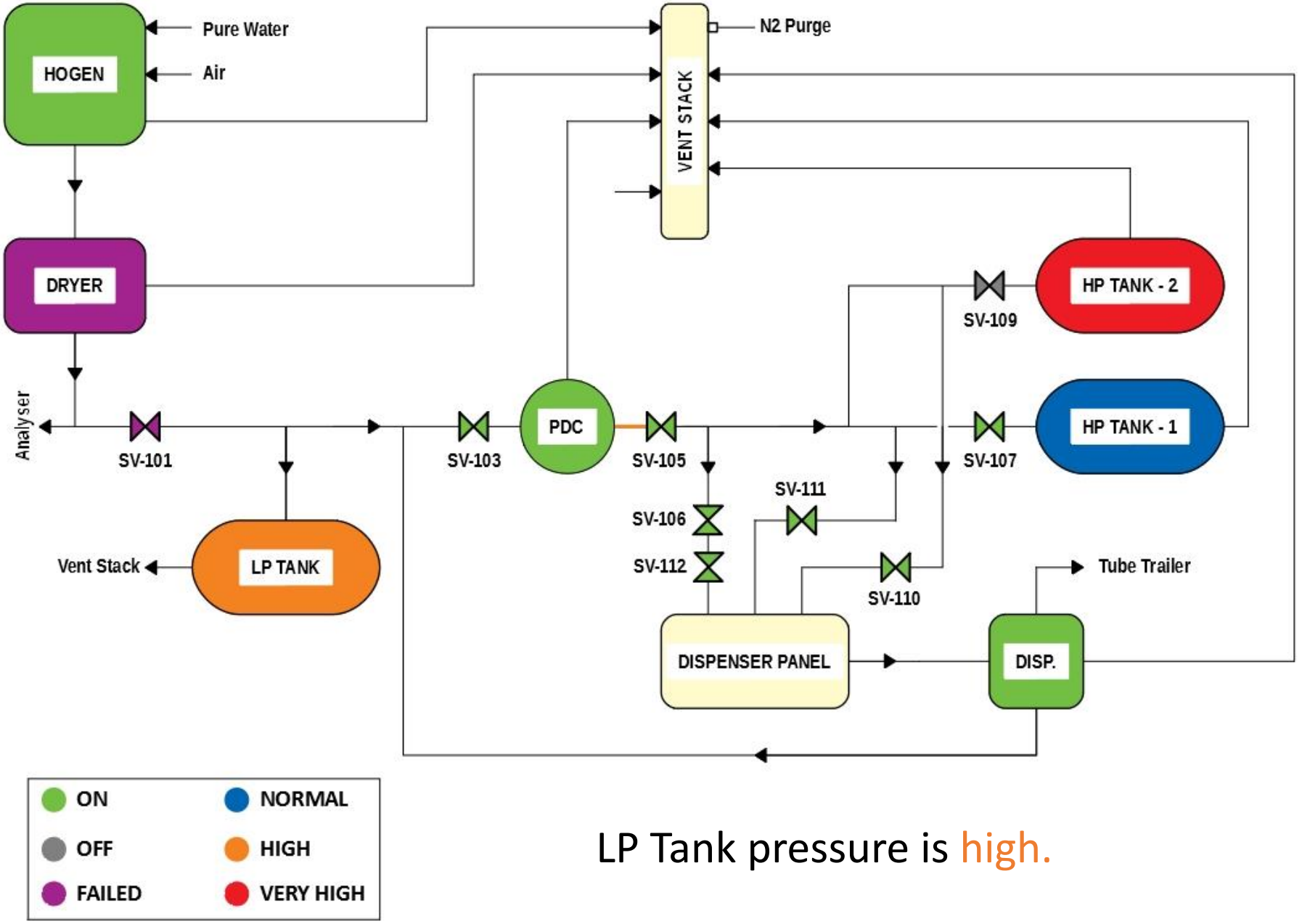
Dryer has a problem.



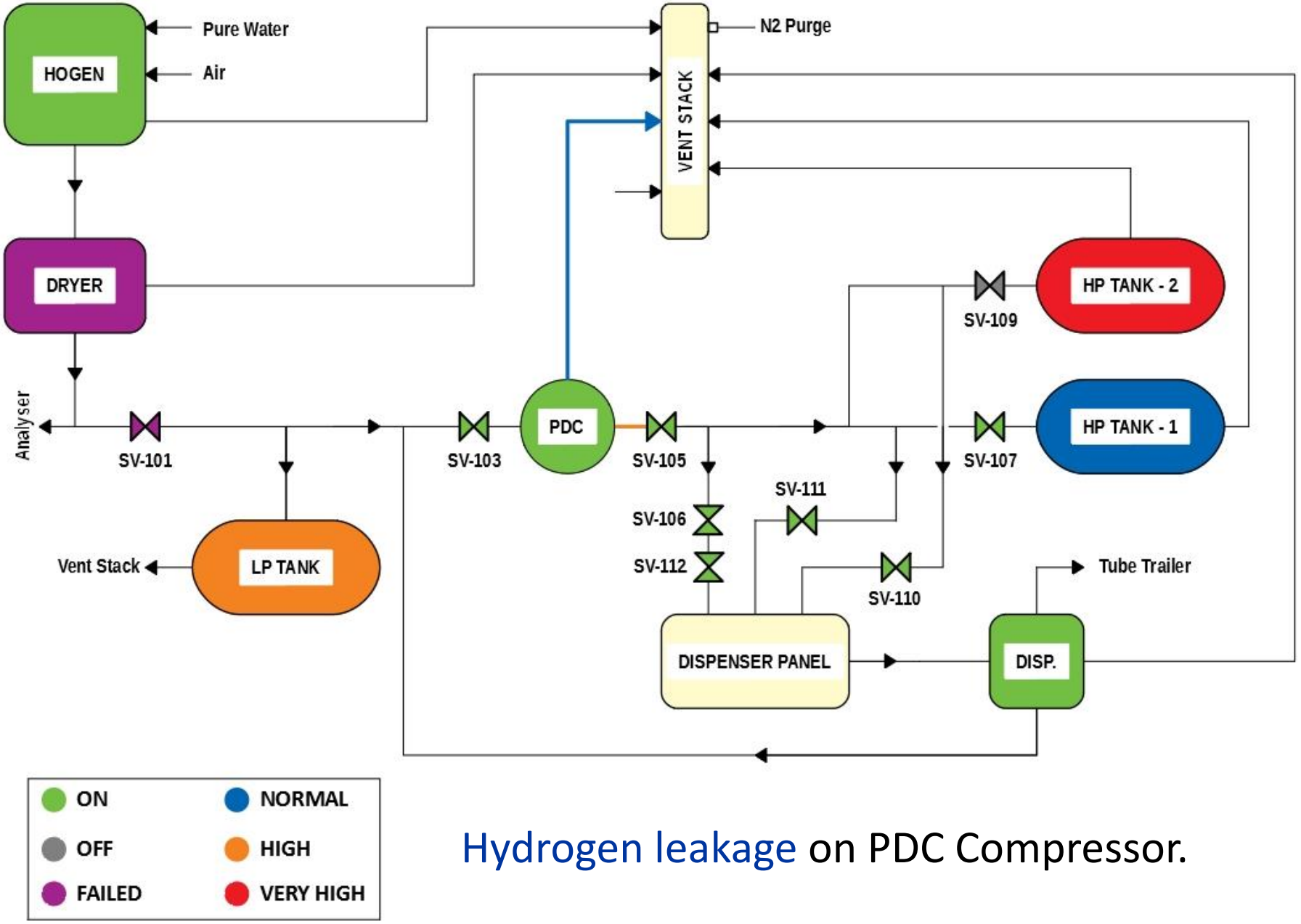
Analyser detected excess water in sample.
SV-101 will be closed.



SV-101 failed to close.



LP Tank pressure is high.



Hydrogen leakage on PDC Compressor.

• ANALYSIS (4/6)

Parameters given to SPIN for verification:

- Physical Memory Available: 6144 MB
- Estimated State Space Size: 8000 (states x 10^3)
- Maximum Search Depth: 1000000 (steps)
- Hash factor: 1

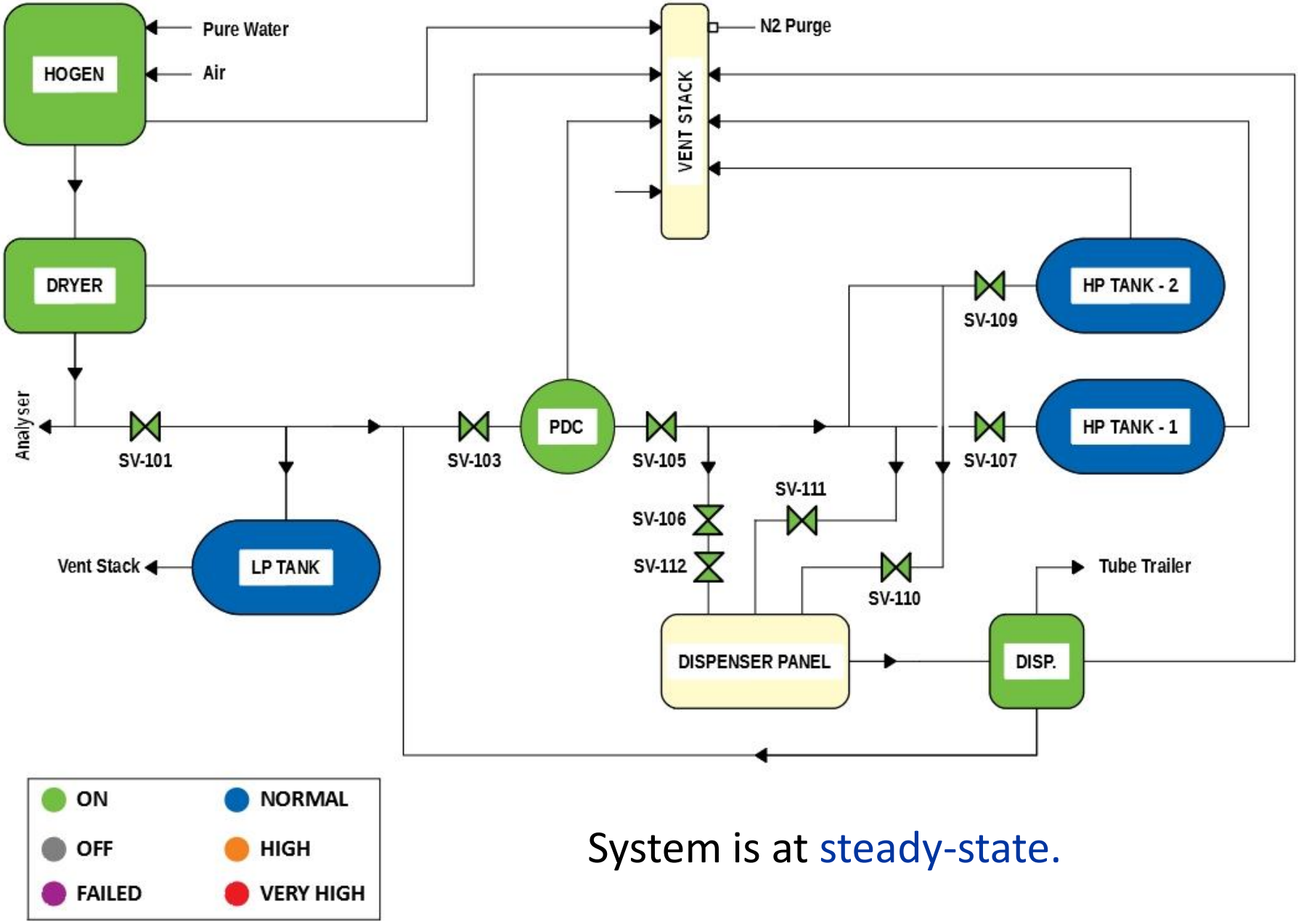
Verification result:

- State-vector: 596 bytes
- Depth reached: 999999
- Errors (counterexample): 1
- Assertion violated at depth 173
- Hash factor: 1.139
- Equivalent memory usage for states: 4324.786 MB
- Elapsed time: 32.6 seconds

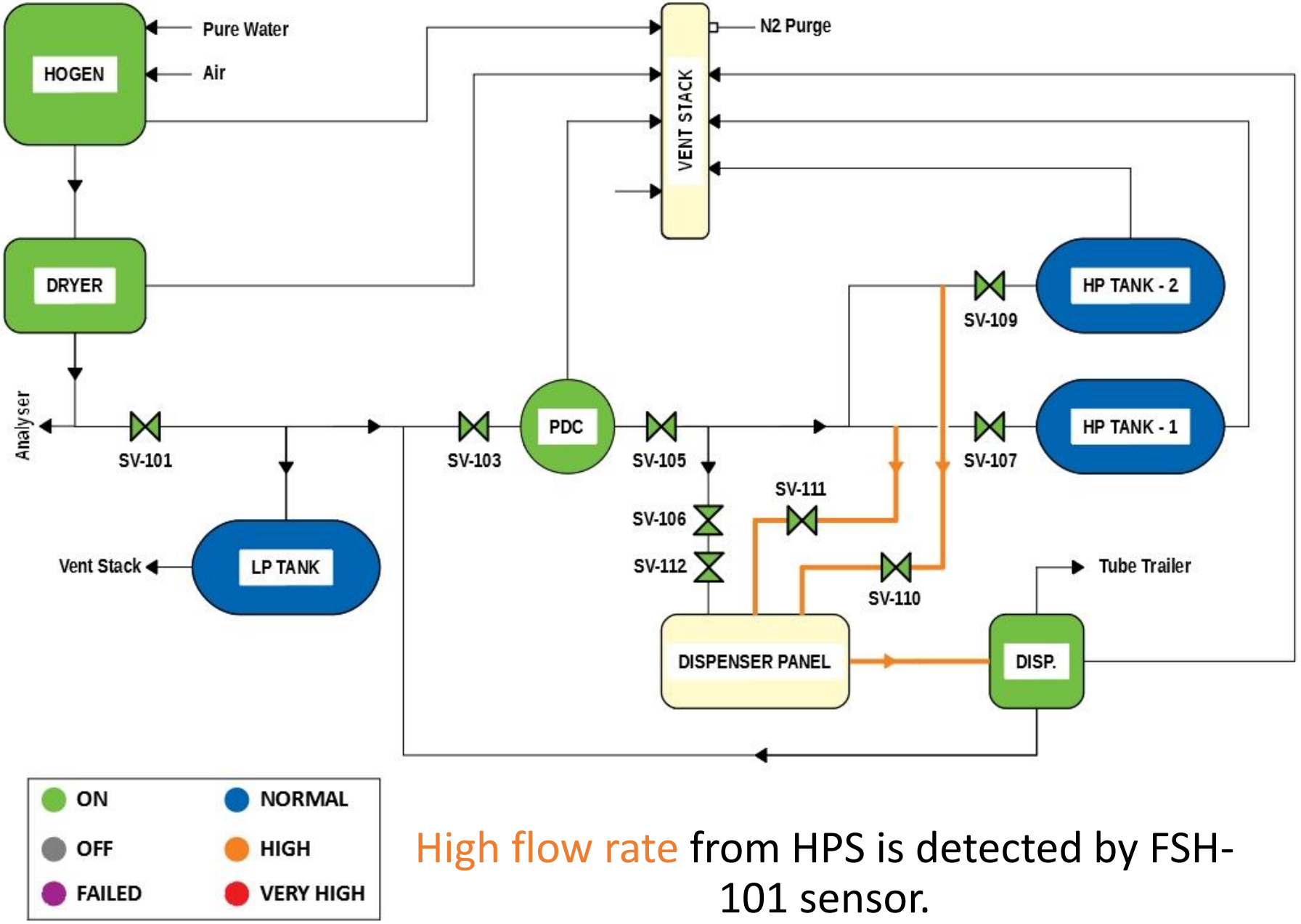
• ANALYSIS (5/6)

- It is found that there are **double points of failure** in the system!
- These failures are **independent!**

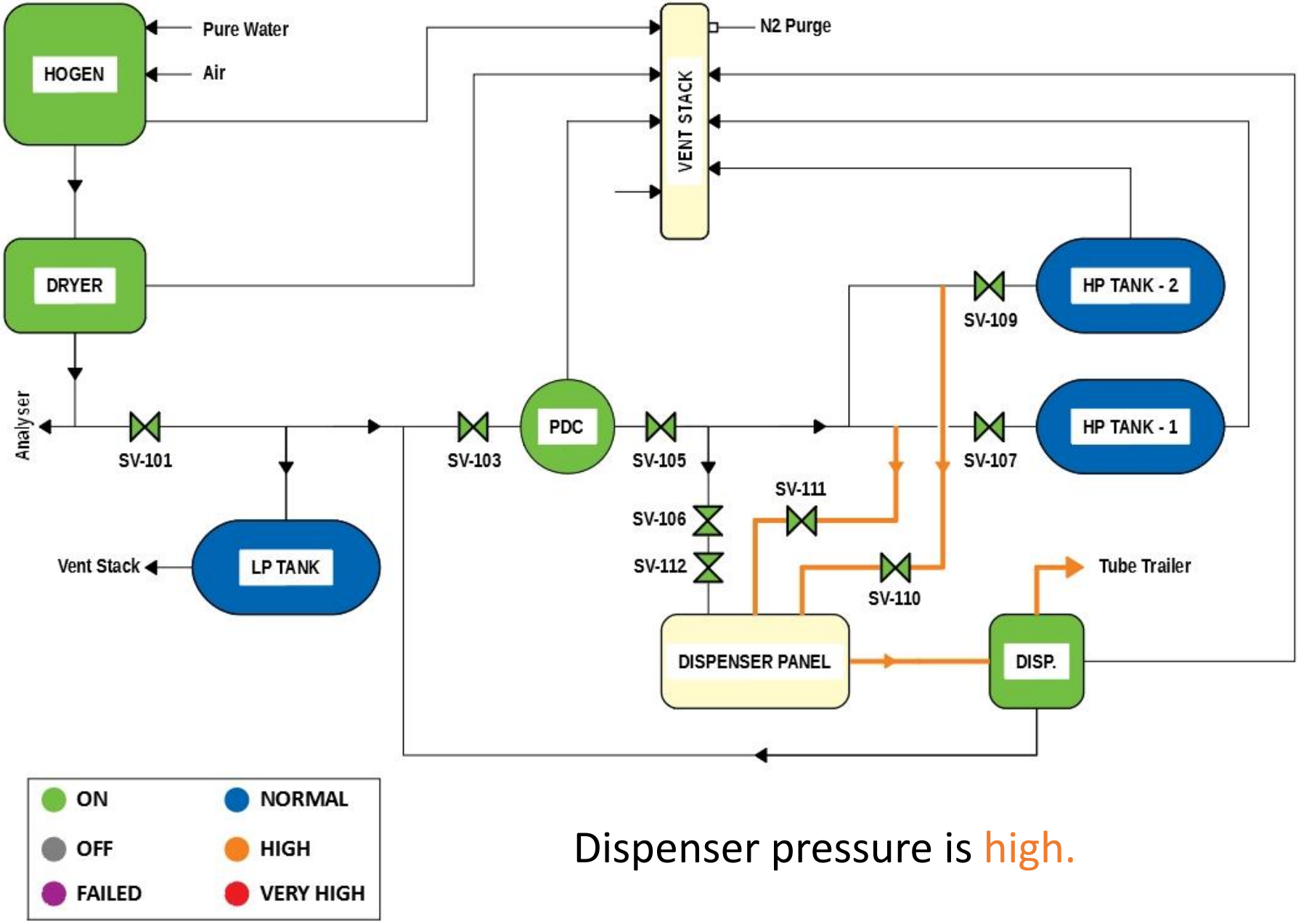
Different scenarios (with different claims) can show PDC Compressor leakage with more points of failure. Next animation gives a different scenario with **4 points of failure.**



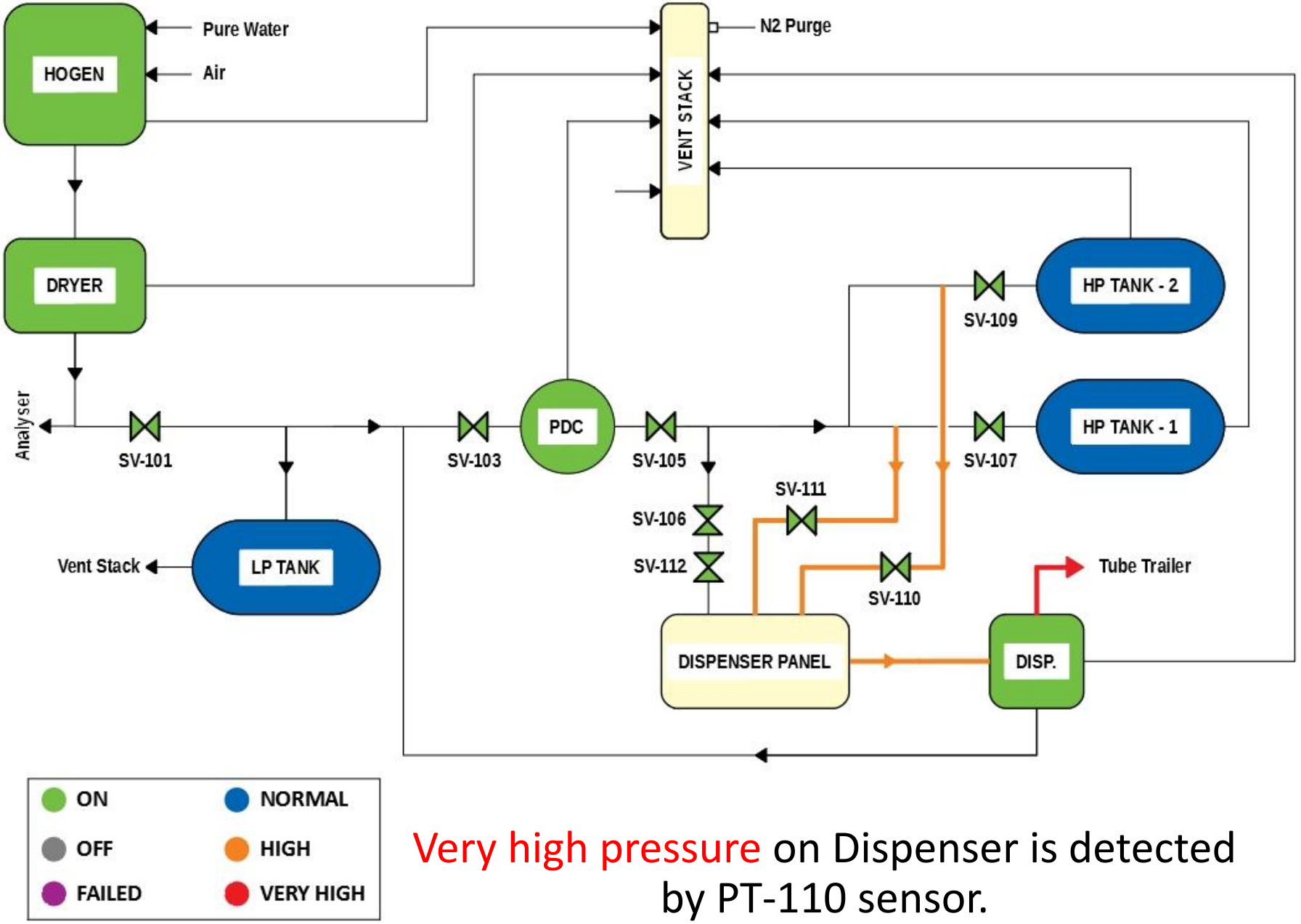
System is at steady-state.



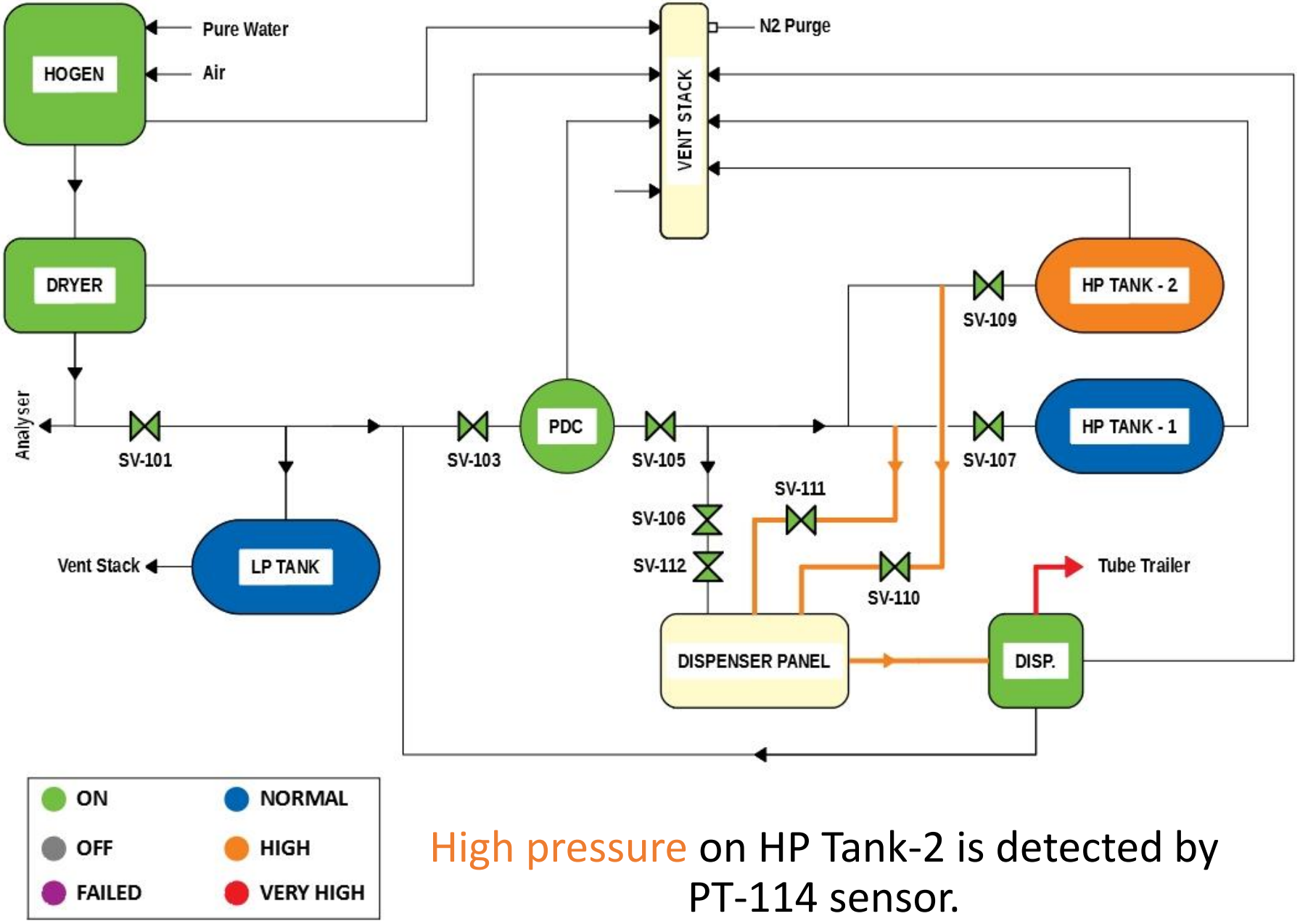
High flow rate from HPS is detected by FSH-101 sensor.



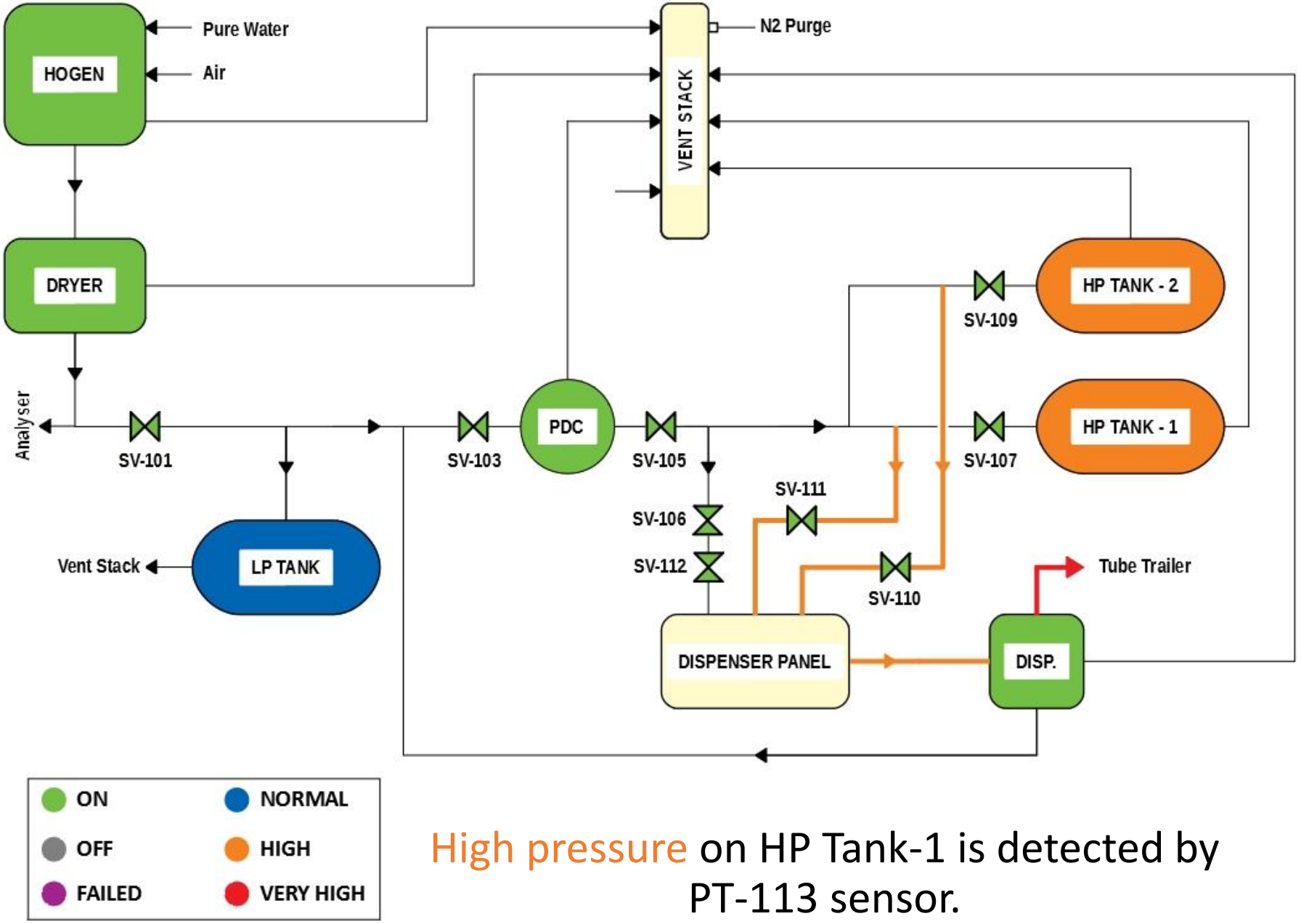
Dispenser pressure is high.



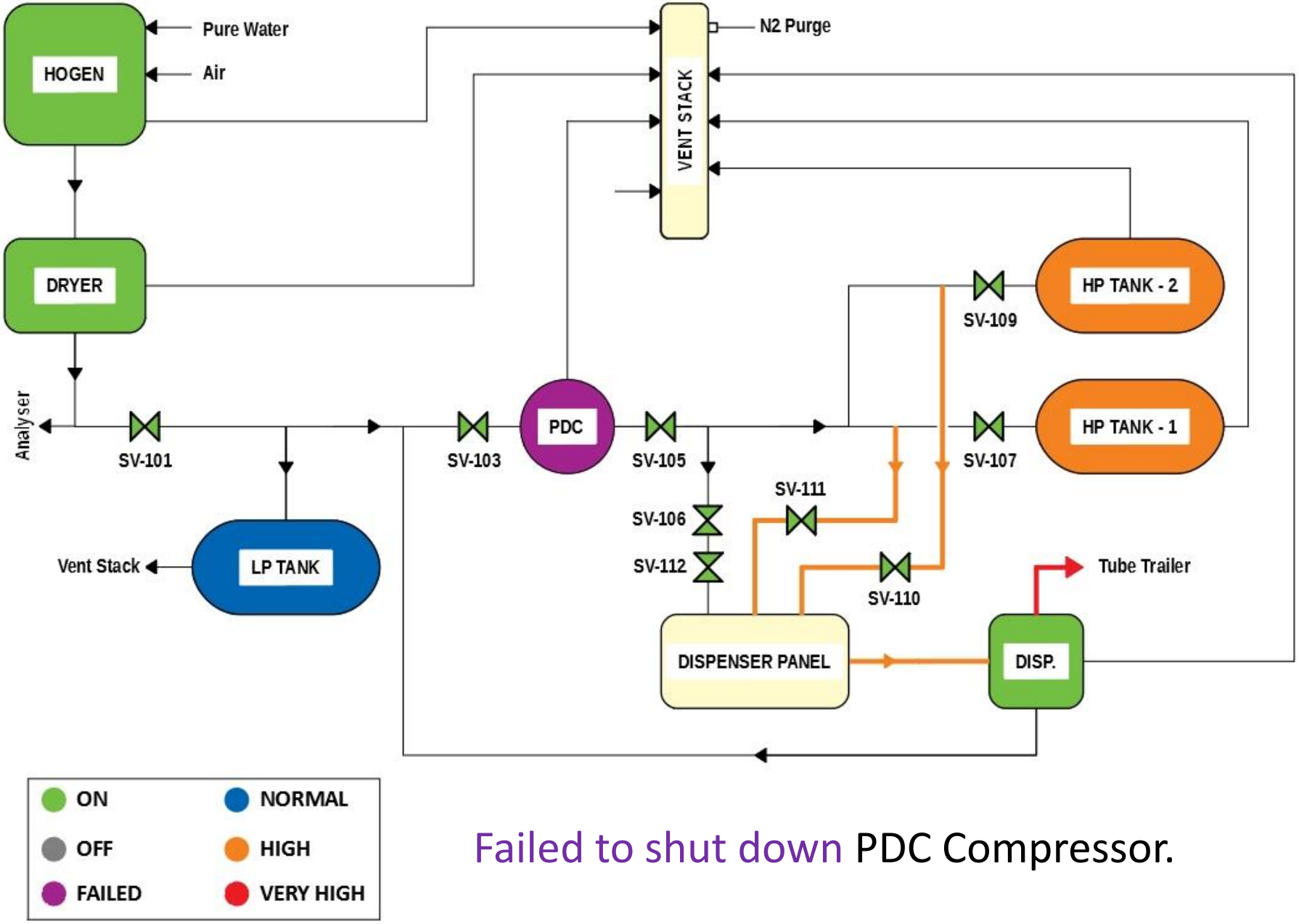
Very high pressure on Dispenser is detected by PT-110 sensor.



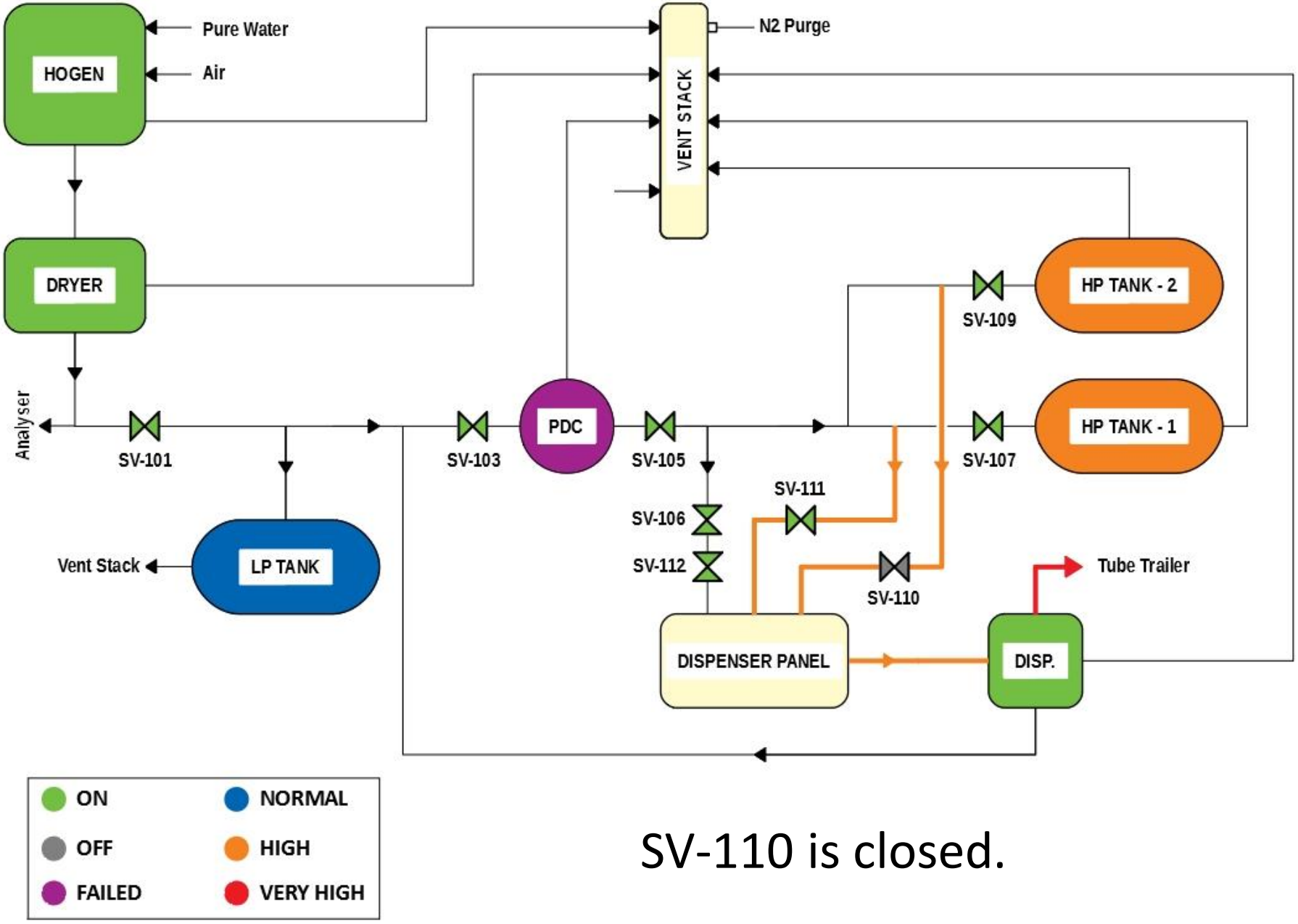
High pressure on HP Tank-2 is detected by PT-114 sensor.



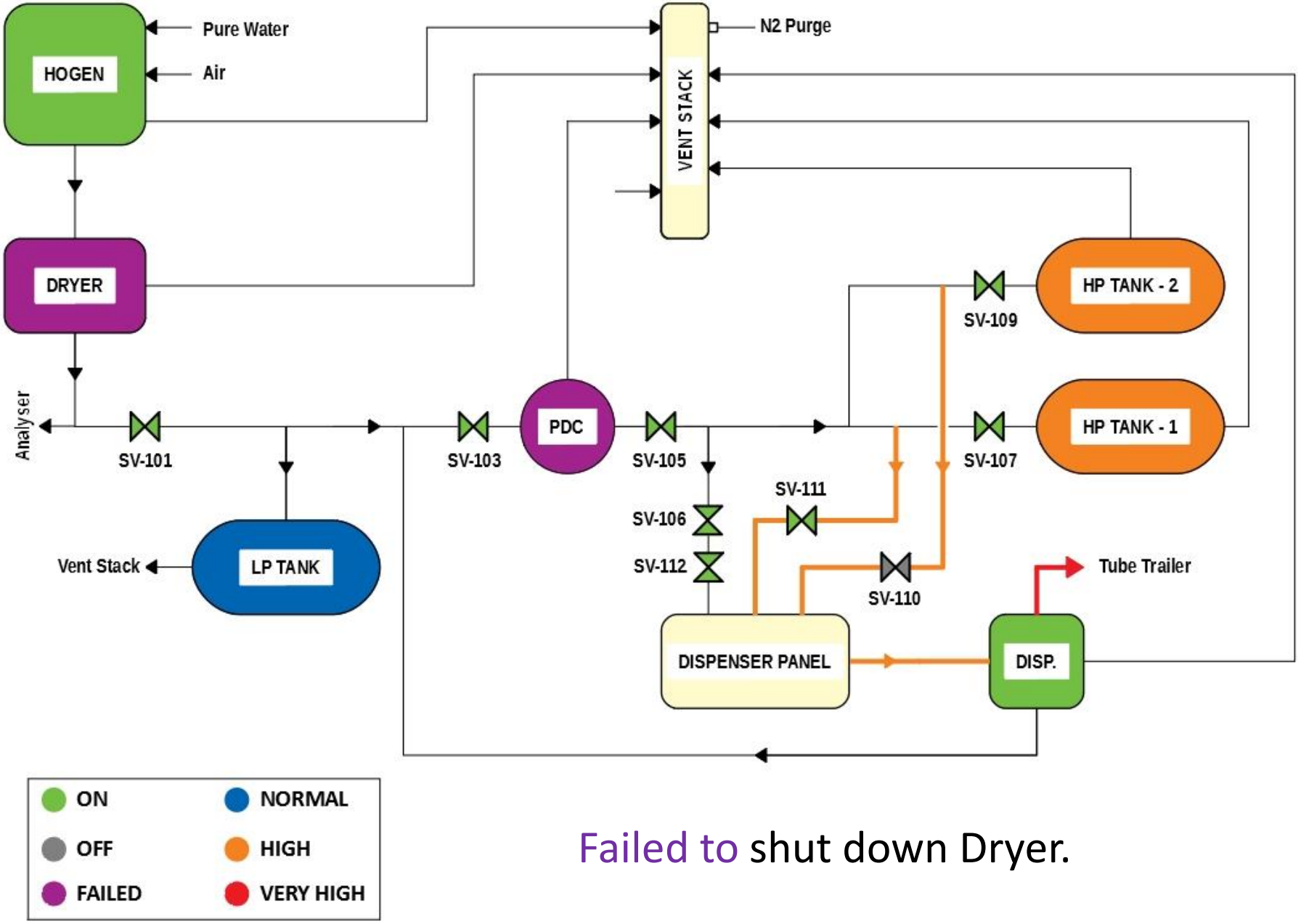
High pressure on HP Tank-1 is detected by PT-113 sensor.



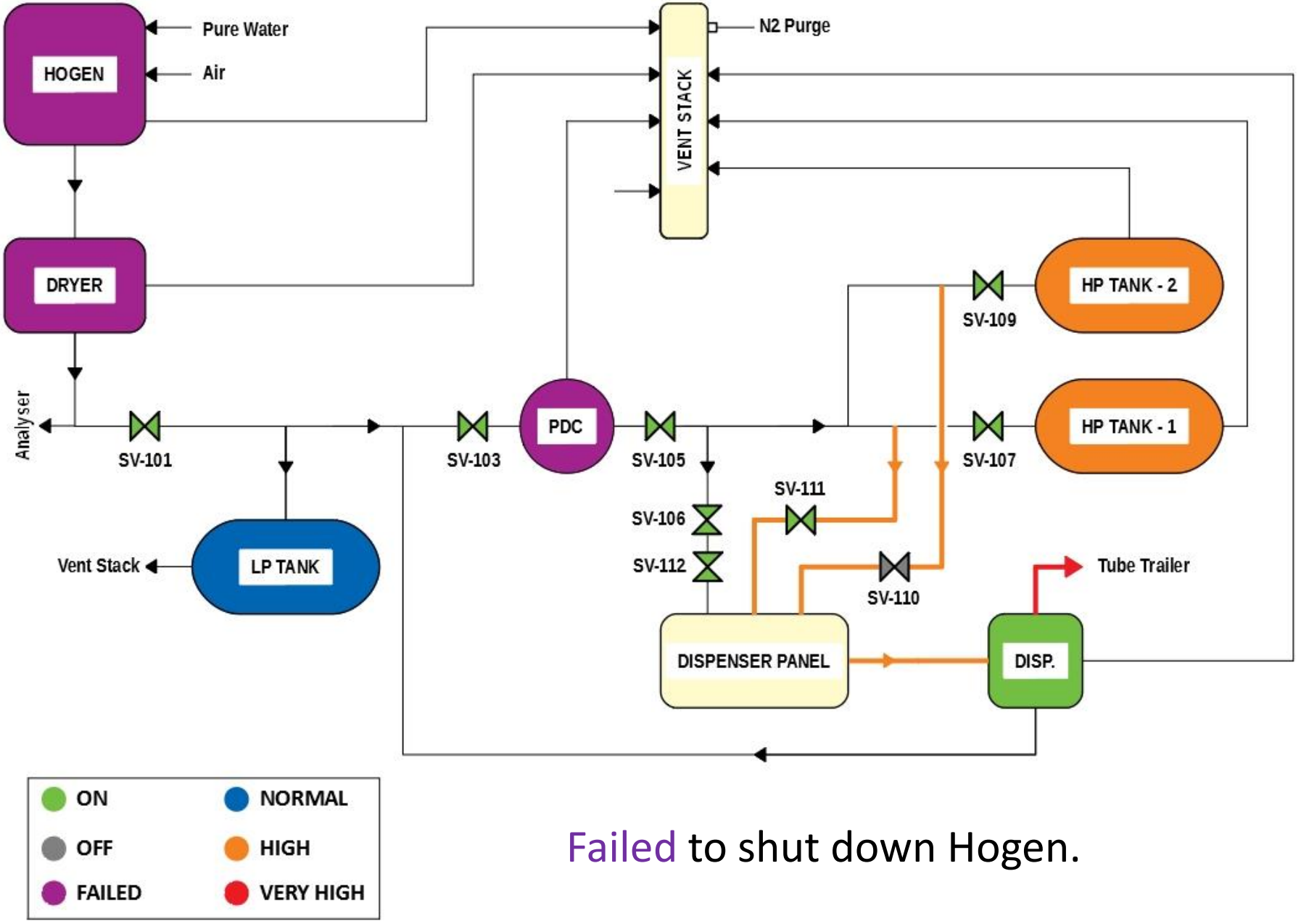
Failed to shut down PDC Compressor.



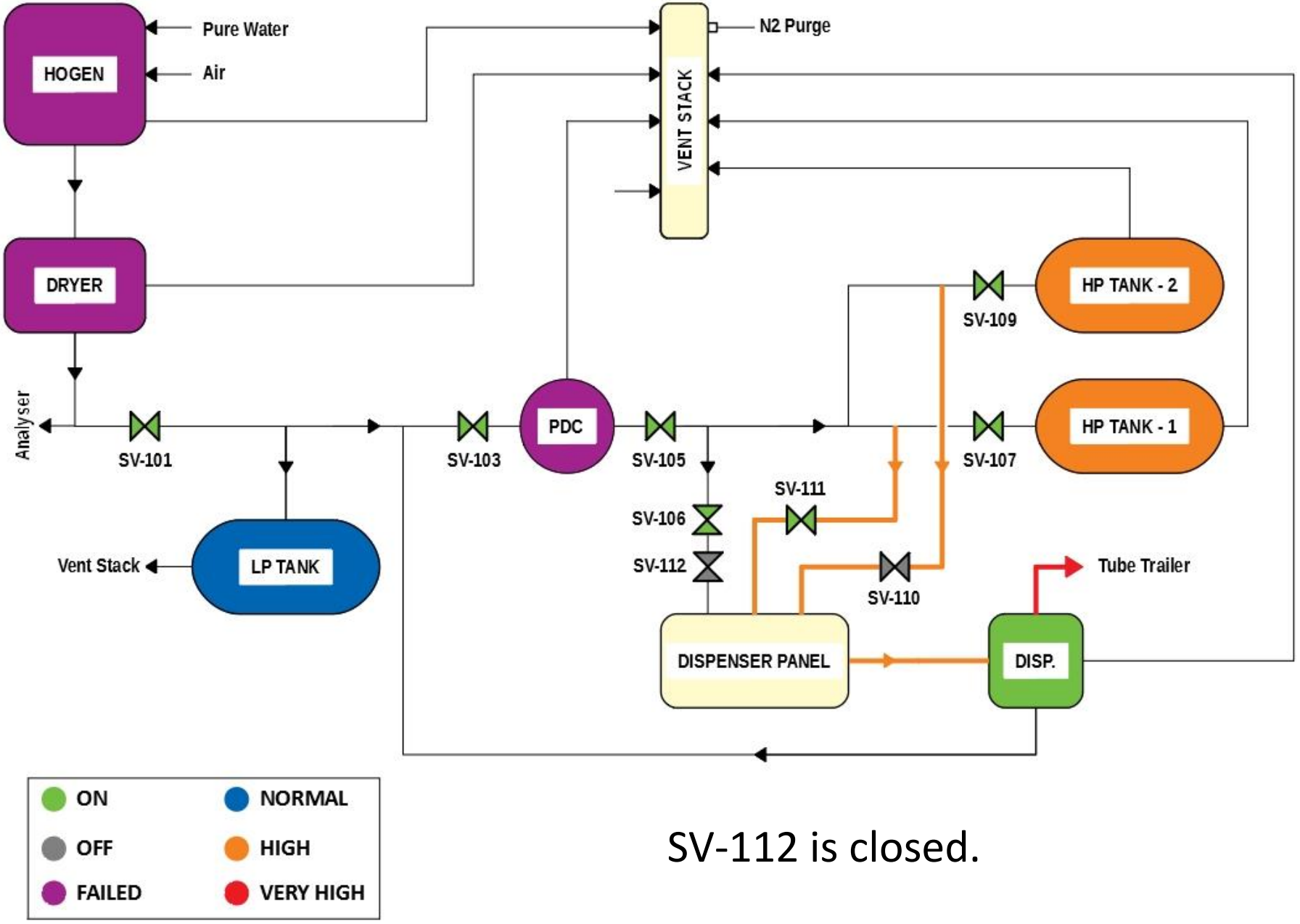
SV-110 is closed.



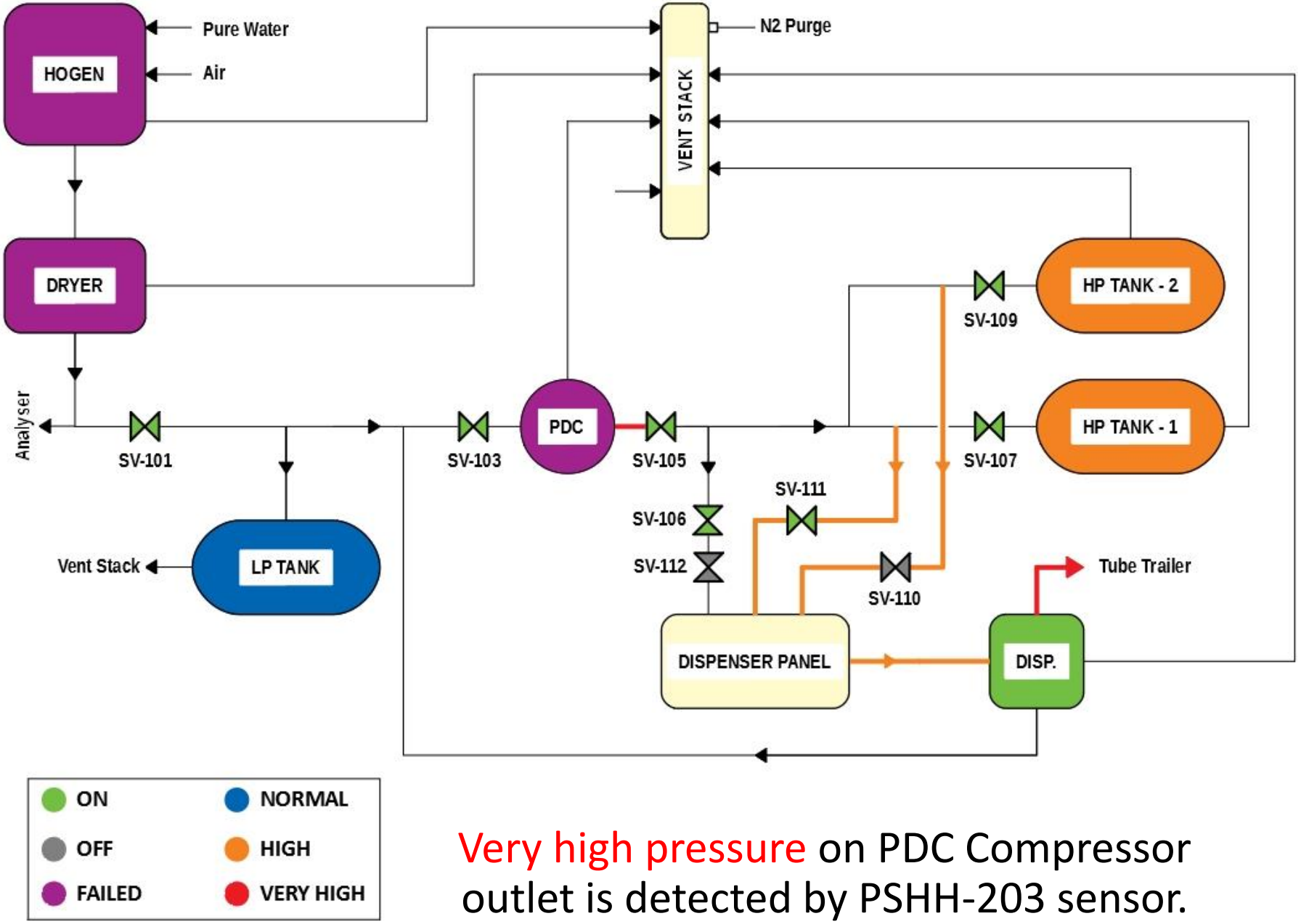
Failed to shut down Dryer.



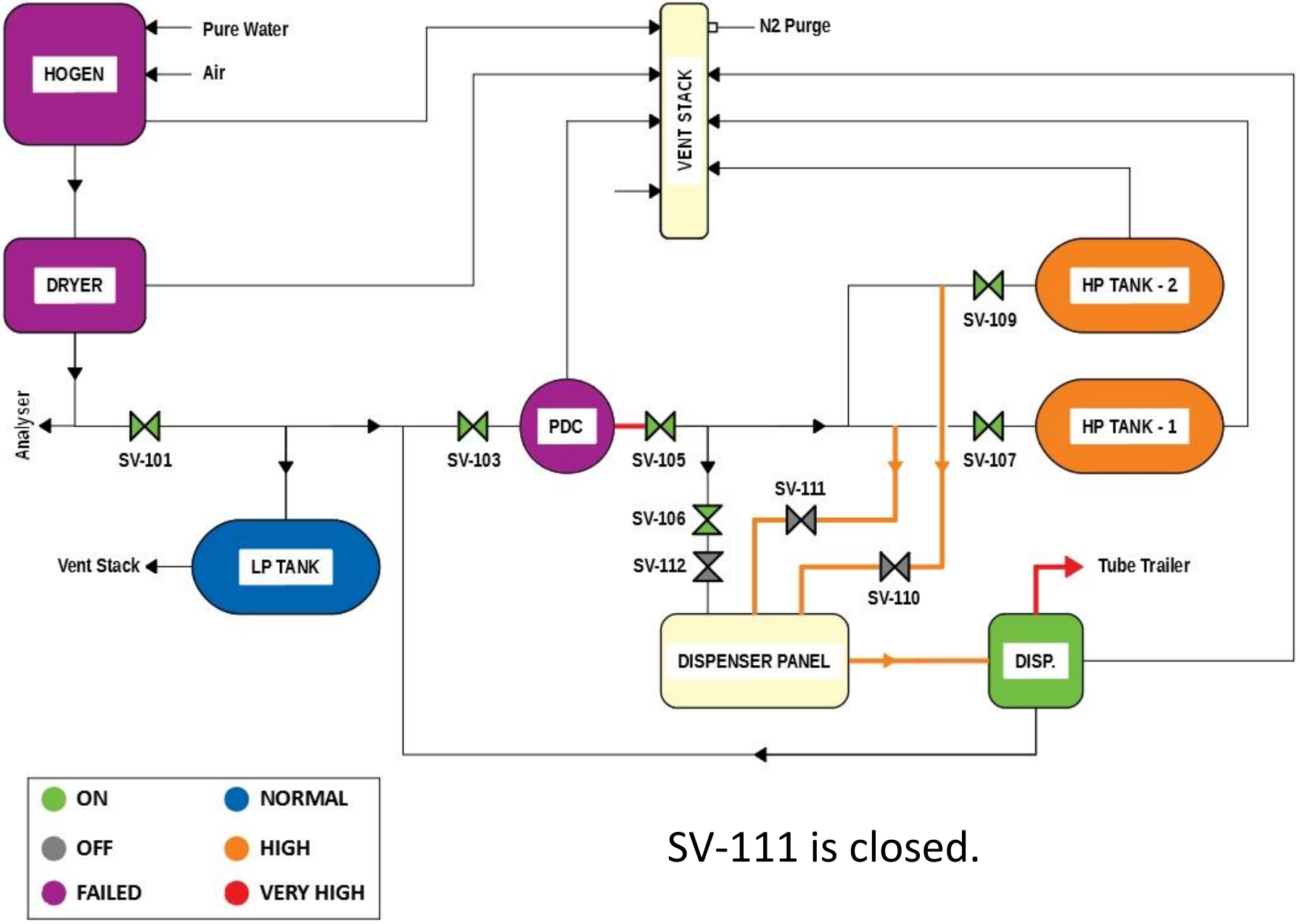
Failed to shut down Hogen.



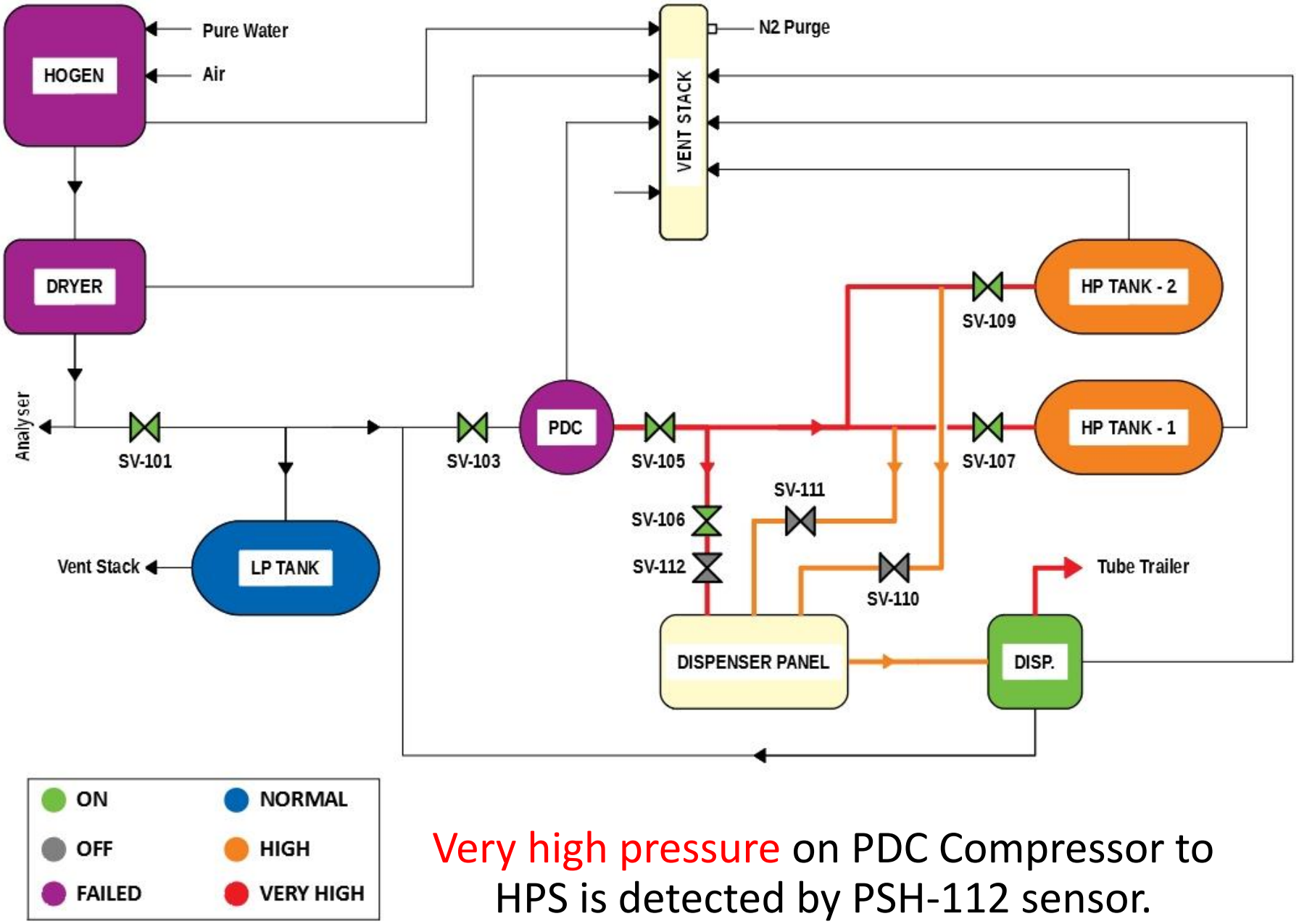
SV-112 is closed.



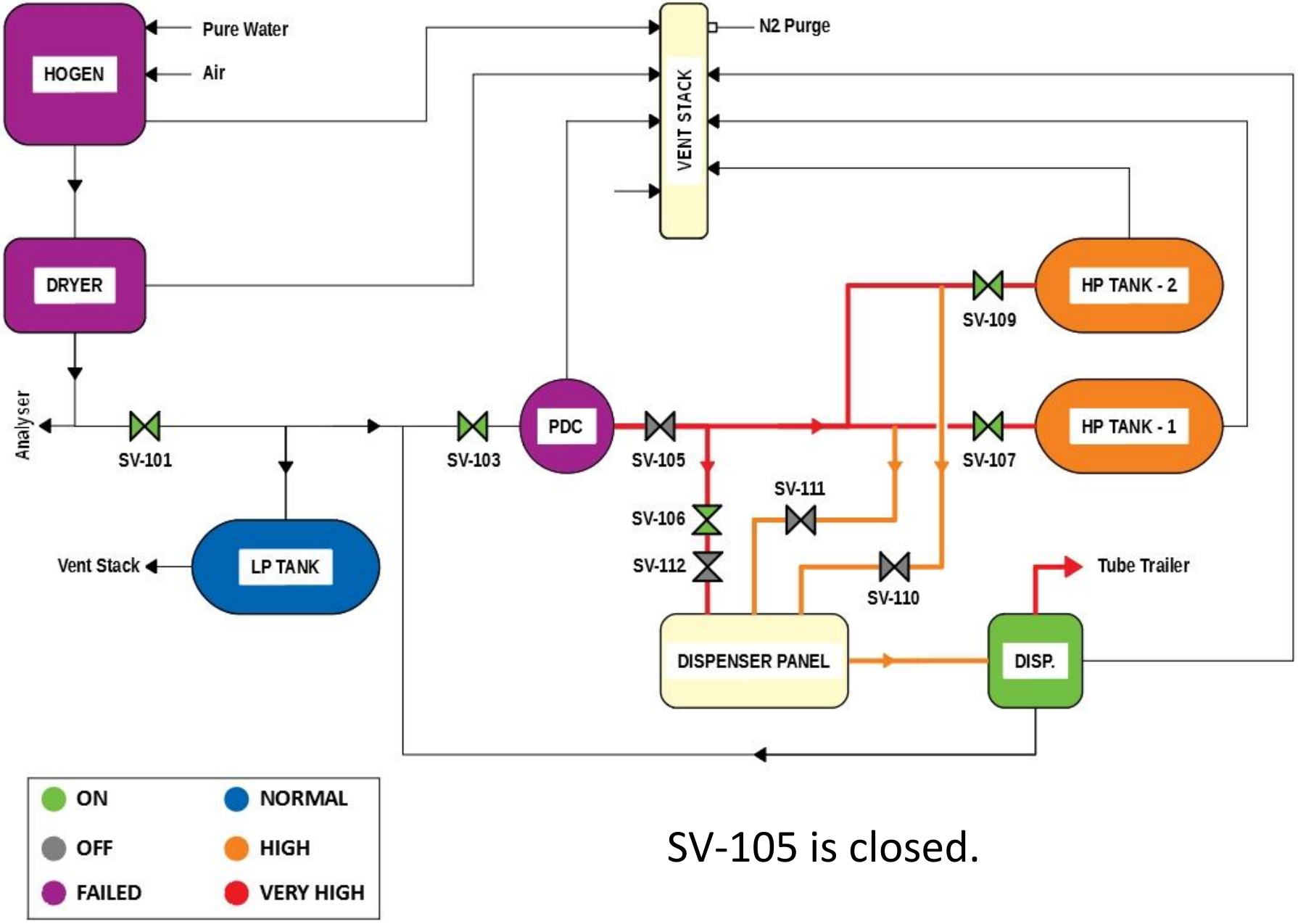
Very high pressure on PDC Compressor outlet is detected by PSHH-203 sensor.



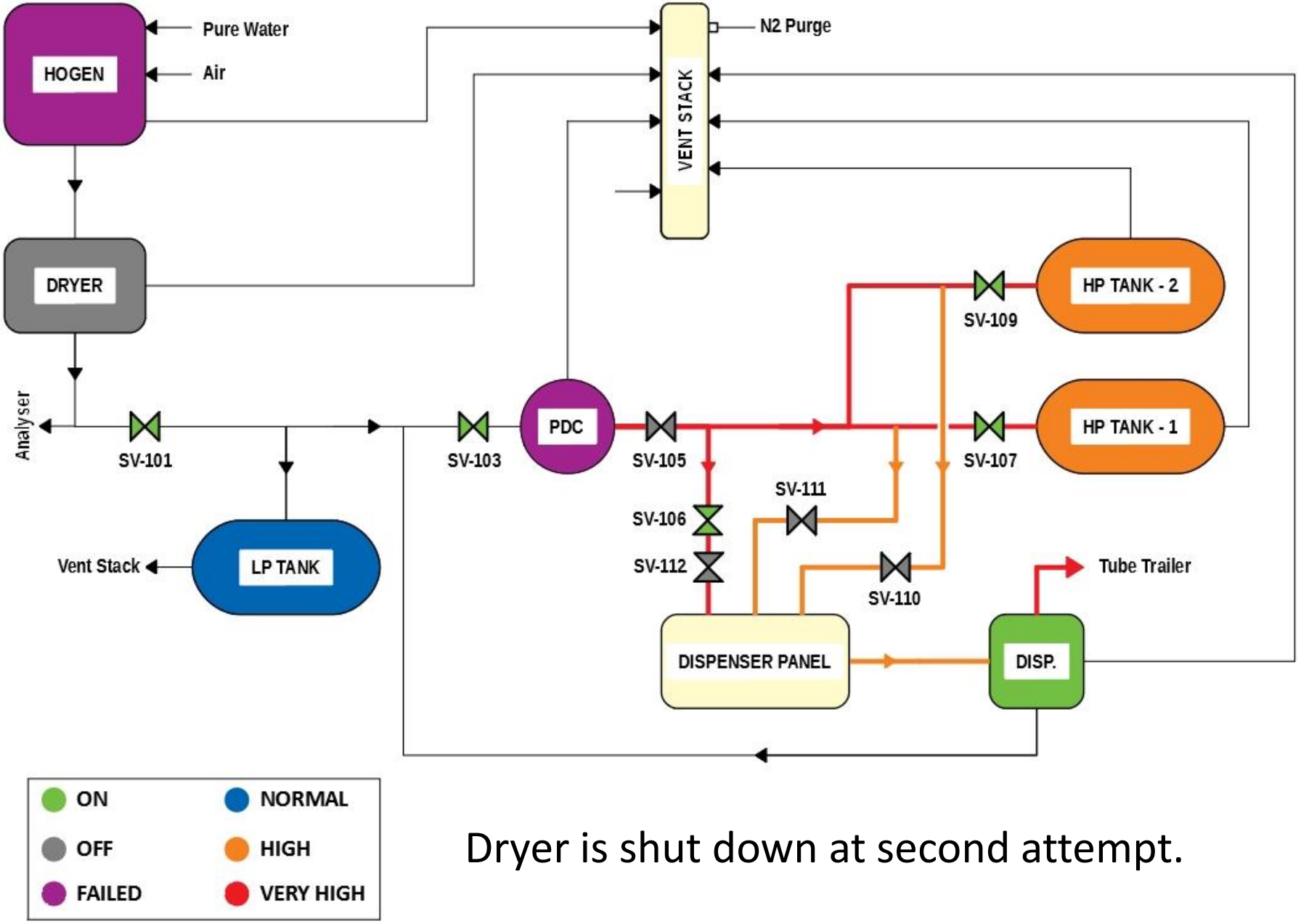
SV-111 is closed.



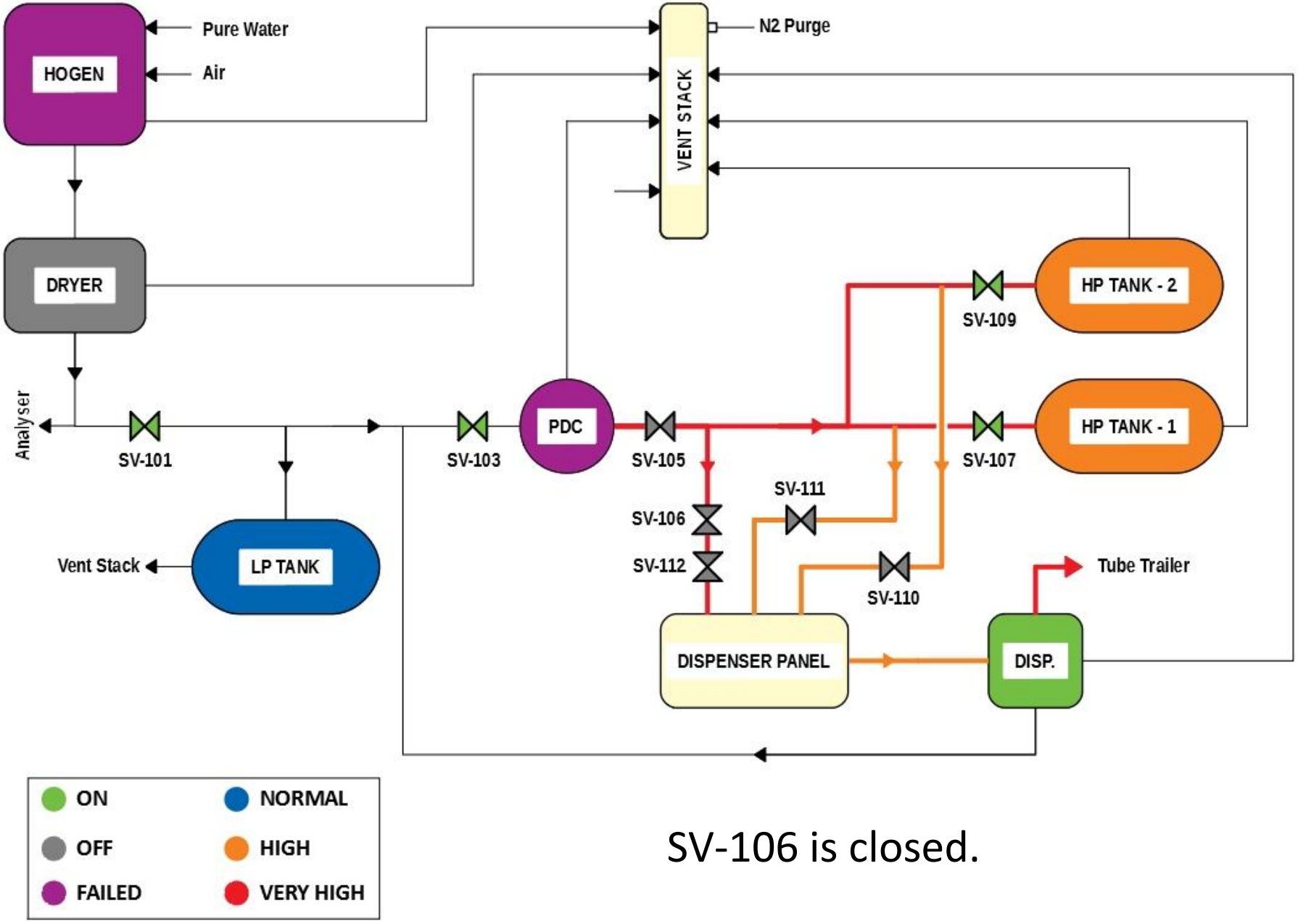
Very high pressure on PDC Compressor to HPS is detected by PSH-112 sensor.



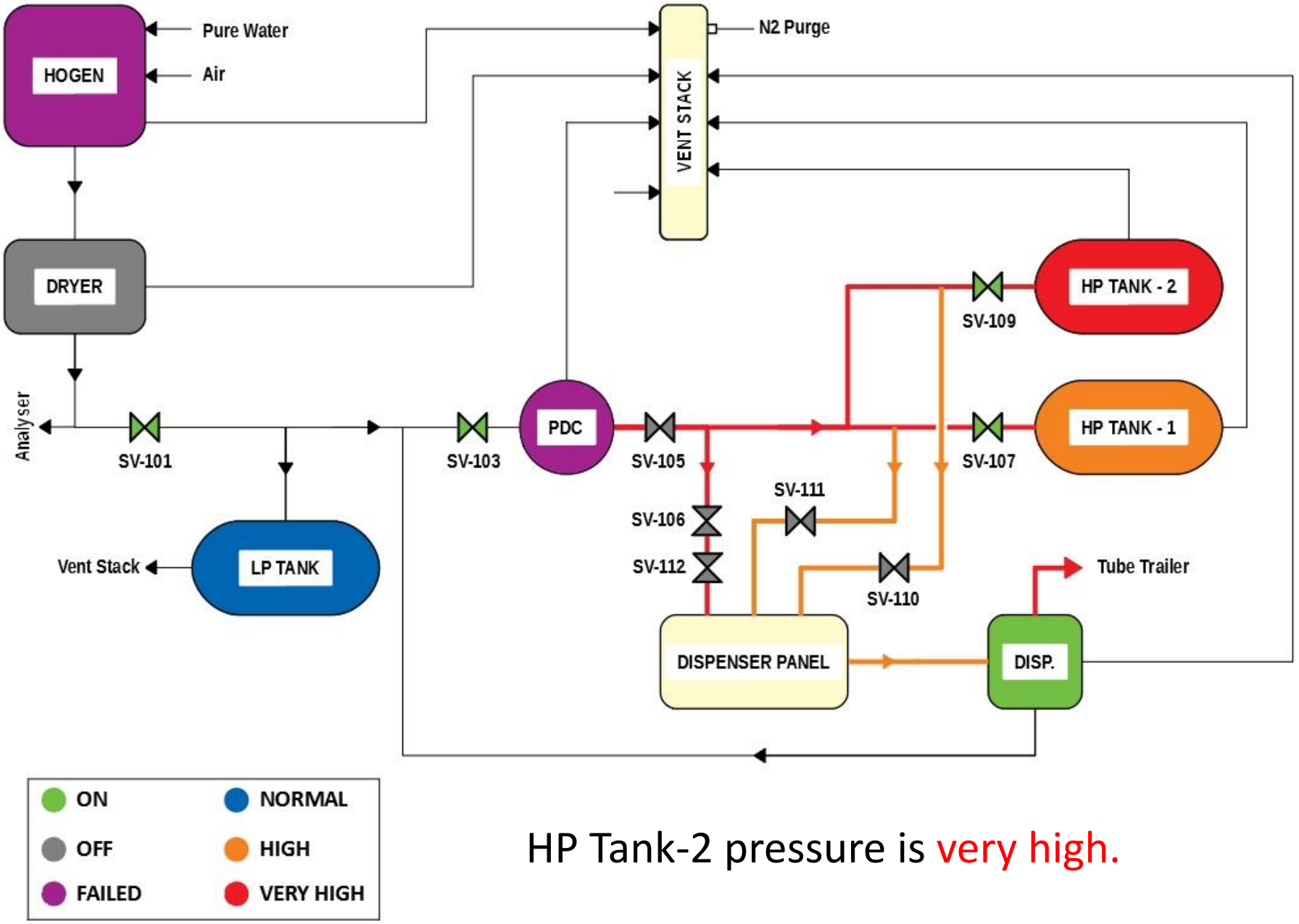
SV-105 is closed.



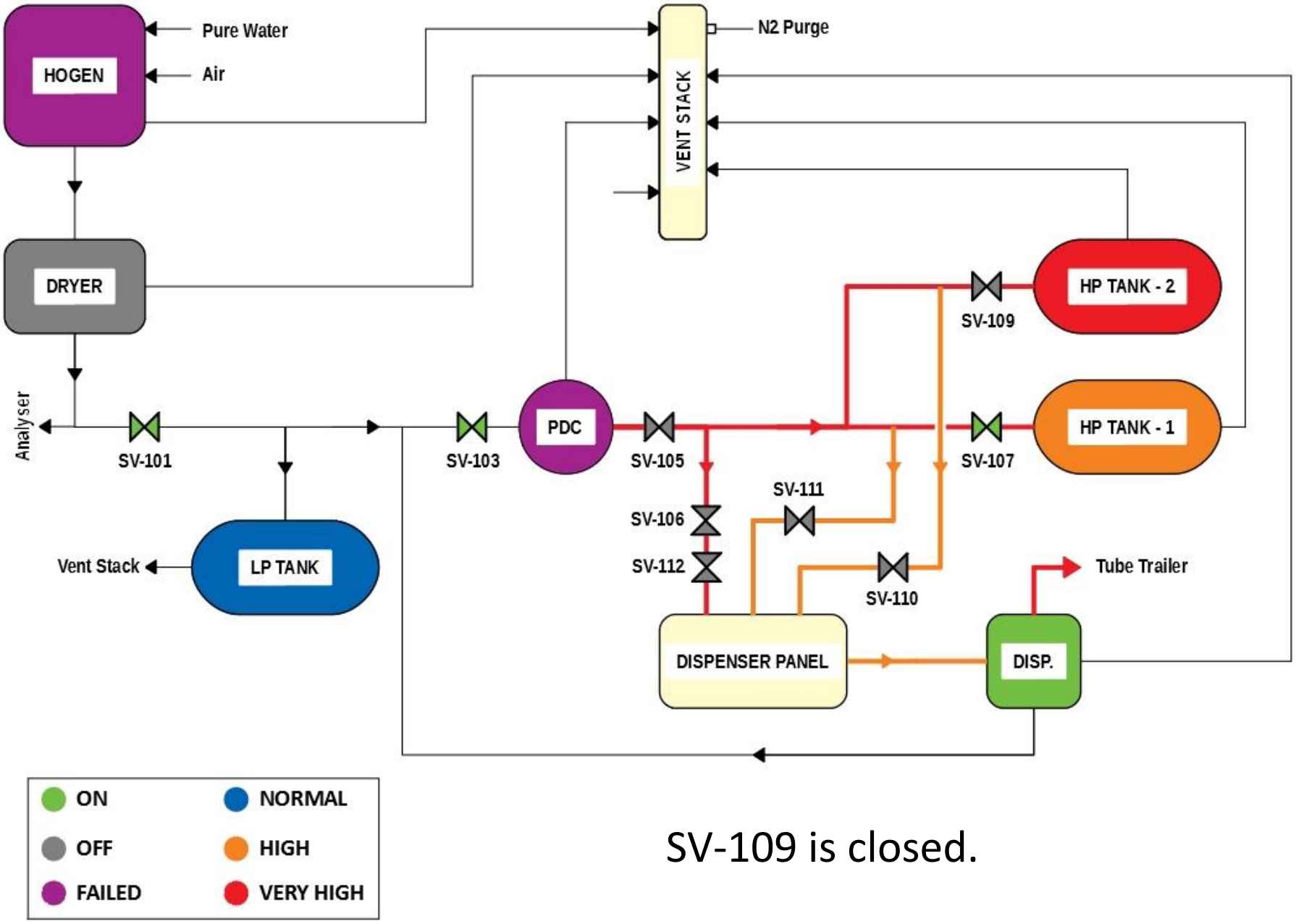
Dryer is shut down at second attempt.



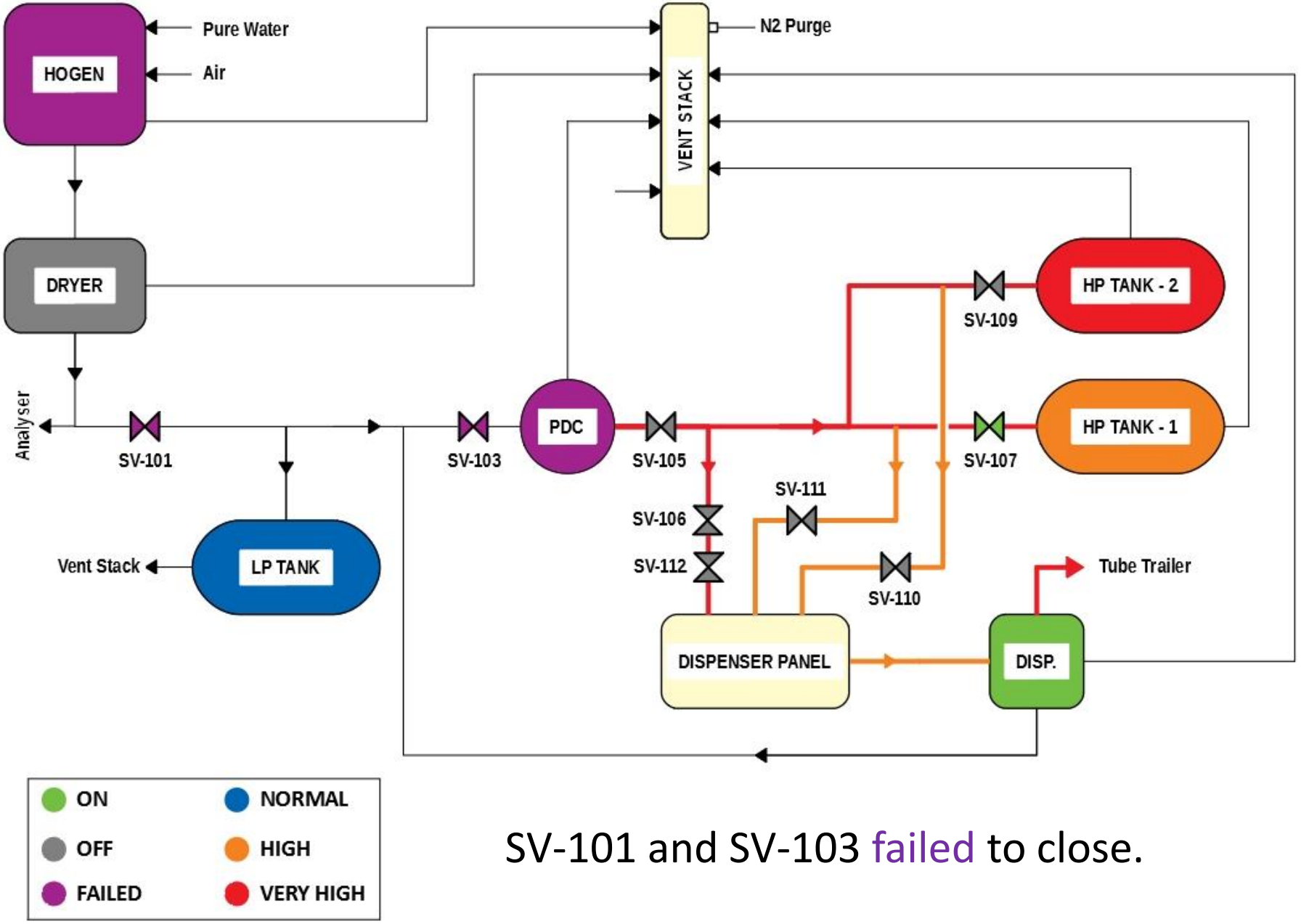
SV-106 is closed.



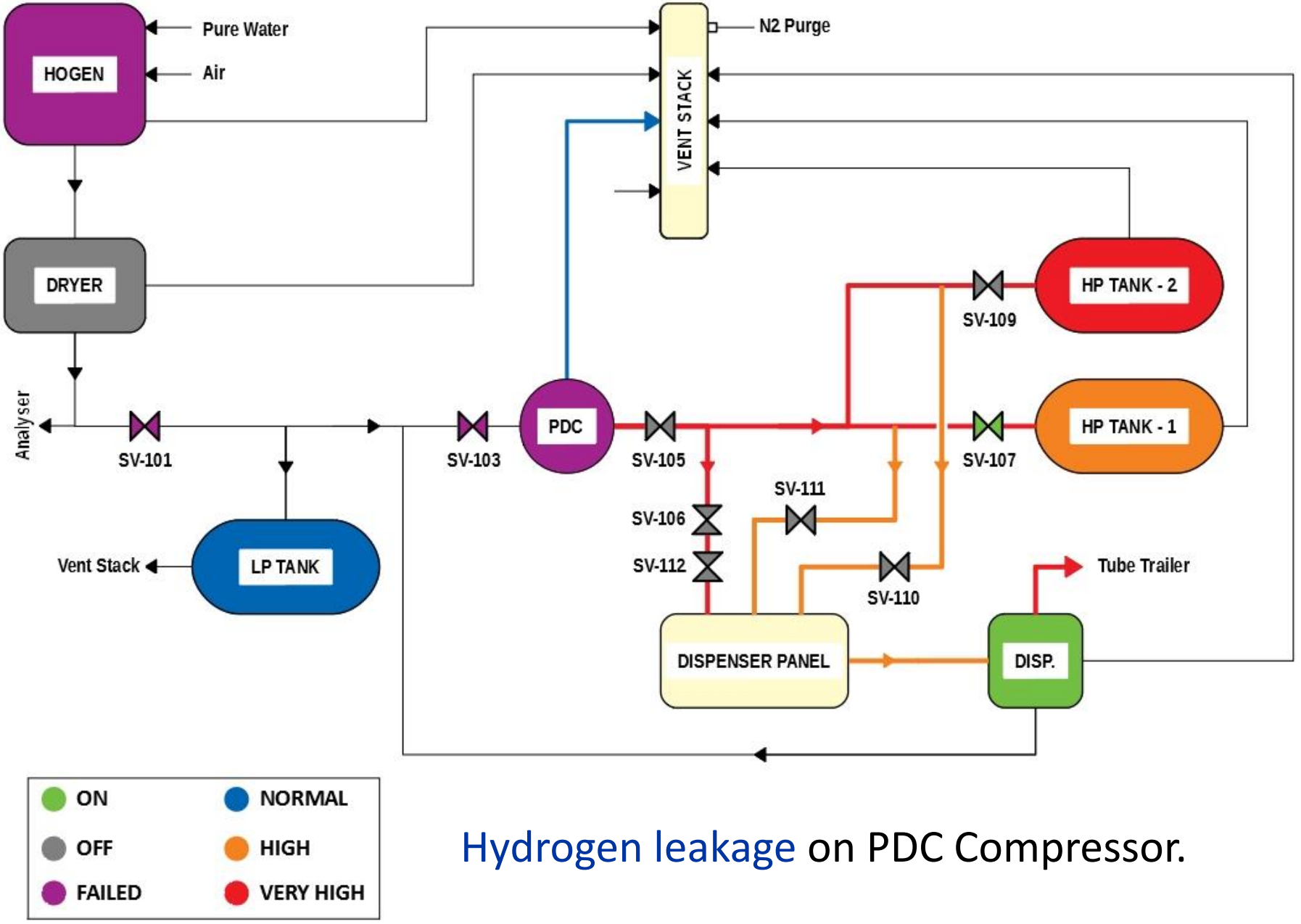
HP Tank-2 pressure is very high.



SV-109 is closed.



SV-101 and SV-103 failed to close.



Hydrogen leakage on PDC Compressor.

• ANALYSIS (6/6)

- Analysis of different states with various claims showed that the system has mostly 4 or more points of failure.
- Fire and pipeline leakage states were found after 10,000 iterations as a result of tracing.
- Many critical states for HP tanks were discovered.
- Safety critical operations that trigger EMS activation were explored.

• CONCLUSION & FUTURE WORK

- Model checking is a fast way to find safety critical states for chemical plants.
- Analyses show that minimum points of failure is 2 for the current system model.

In order to improve the system model:

1. Time dependence.
   - All processes can be prepared as time dependent.
2. Probabilistic approaches.
   - Any event can occur with a pre-defined probability.

   (e.g. which events are most likely to occur?)

• REFERENCES

1. Karner D, Franchfort J. Arizona Public Service – Alternative Fuel (Hydrogen) Pilot Plant Design Report. INEEL/EXT-03-00976.
2. Mazloomi K, Gomes C. Hydrogen as an energy carrier: Prospects and challenges. Renewable and Sustainable Energy Reviews 16 (2012) 3024– 3033.
3. Air Liquide. Storing Hydrogen. Retrieved from https://energies.airliquide.com/resources-planet-hydrogen/how-hydrogen-stored.
4. National Aeronautics and Space Administration. System Failure Case Studies. Vol. 2 Special Issue. Jan 2008.
5. Ben-Ari M. Principles of the Spin Model Checker. Springer, 2008.
6. Brinksma E, Mader A. Verification and Optimization of a PLC Control Schedule. 7th International SPIN Workshop, Stanford, CA, 2000.


THANK
YOU