UNREVEALED FAILURES OF SAFEGUARDS

IMPROVING AND UNDERSTANDING FUNCTIONALITY

KAY A. MODI
JCL RISK SERVICES LLC

PHA Safeguards: Maintaining Their Integrity

Unrevealed failure: no system monitoring the failed state condition of a safeguard and the failed state can be for an extended period

If Ability to Perform Maintenance or Function Test is Limited,

Is the safeguard effectiveness insufficient ?

Procedures or Critical Tasks Used as Safeguards

need to be audited (quarterly?, documented?)

Well formulated safeguards may need to include notations on how to maintain their integrity (add pressure monitoring downstream, add annual change-out, or add quarterly audit by supervisor)

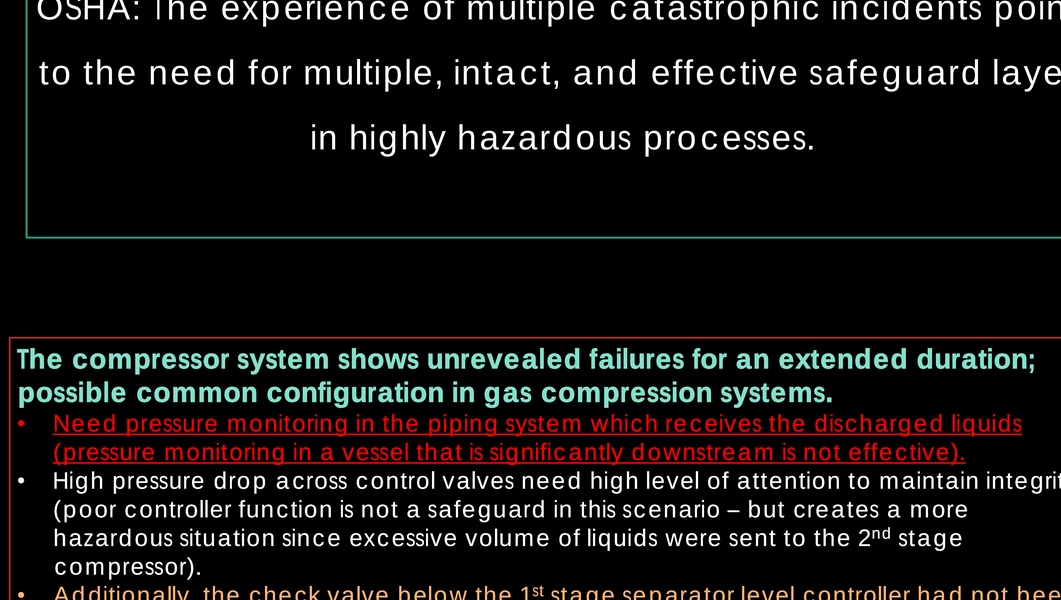
Double Jeopardy: two REVEALED failures

Without common cause that would only have a short duration of failure before being detected

OSHA: The experience of multiple catastrophic incidents points to the need for multiple, intact, and effective safeguard layers in highly hazardous processes.

The compressor system shows unrevealed failures for an extended duration; possible common configuration in gas compression systems.

- Need pressure monitoring in the piping system which receives the discharged liquids (pressure monitoring in a vessel that is significantly downstream is not effective).
- High pressure drop across control valves need high level of attention to maintain integrity (poor controller function is not a safeguard in this scenario – but creates a more hazardous situation since excessive volume of liquids were sent to the 2nd stage compressor).
- Additionally, the check valve below the 1st stage separator level controller had not been maintained and did not prevent liquid backflow (safeguard?).
- These issues contribute to the ineffectiveness of the 1st stage level controller preventing liquids from entering the 2nd stage compressor when an initiating cause of "composition change of higher MW gas due to unit upsets or change in operation" occurs.
- ***Safeguard well formulated: BPCS that are not readily understood by operations as working appropriately may need continual downstream monitoring (add pressure transmitter) or other means to assess effectiveness.***

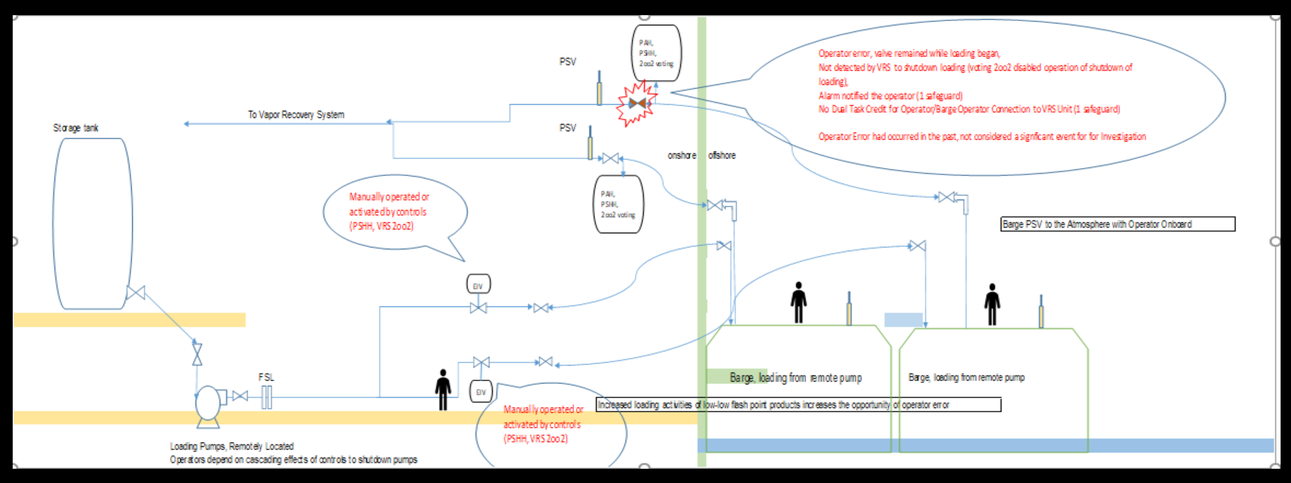


ARe your Safeguards Functional?

Pre-Engineered Systems:

1st Issue: Interlocks - For safety or for operation preferences in the voting design? **

Did the PHA review the details of voting issues of Safeguard?
Operators noted that the VRS did not shutdown on one valve misalignment but did not complain due to long term operating issue (system used for 12 years)
Was the safeguard audited?
When a safeguard does not work as intended, is it a near miss and properly investigated or does it become a normalized operator's understanding of the equipment design intent?



2nd issue: Lack of Safeguard Audit on Loading Systems (audit task activity, demand rate on SIF)

Operating procedure (noted as critical task) for loading required operator to manually shutdown the pump to complete load (listed as PHA Safeguard credit for checklist that required the operator to turn off the pump before closing EIV, critical task safeguard), but practice became reliance on the pump SIF to shutdown on low flow.

- Lack of following procedures created high demand on the pump SIF to a daily demand function which was not included in the SIF design. Safeguard was not audited **(demand rate)** to assure it was effectively preventing the consequences.
- High pump seal failure rate due to frequent deadhead of pump.

Facility did not include pump seal failure in incident investigation procedure (was the seal life unusually low which would not meet the assumption of a 1/10 year failure rate for initiating cause in PHA ?). **Proper investigation would lead to audit of operator activities – were they following the steps of the critical task safeguard?**

Unrevealed Failures of Block Valves or Check Valves

Due to Lack of Functional Testing

- Examples of unrevealed failures include an emergency block valve being stuck in the open position (had not been closed in years; **for a safeguard listing it should be stroked once per quarter?**) or
- Check valve being stuck in the open position which is unrevealed due to normal forward flow (and no routine testing of effective operation based per its demand cycle).

This highlights the importance of periodically performing functional tests of standby safety critical equipment including check valves (required if used as a safeguard, must be periodically audited to maintain effectiveness).

Collapsed Storage Tank Due to Vacuum

Emptying a tank that has one blank gas regulator to maintain air-free atmosphere during withdrawal:

- vacuum breaker did not work (near its end of life or near the 5-year test cycle) and
- regulator had not been maintained on an annual basis (and/or did not have a backup with routine change out schedule to maintain integrity of the safeguard)
- ***Safeguard well formulated: Regulators that are not readily understood by operations as working appropriately may need quarterly check with visual flow rotameter or backup regulator or annual changeouts (specify in safeguard listing)***

NOT DOUBLE JEOPARDY !

** Notation on skid units: Voting of "pre-engineered system" needs to be defined on P&IDs (notations) if used as a safeguard, since PHA teams may not always have the detailed instrumentation designs available. Skid units are more common in facilities and many are engineered for maintaining operations instead of shutting down more frequently as a safe state priority.
Detailed reviews have found older systems which require 6 out of 6 or 2oo2 when monitoring different connections to skid units (multiple vapor recovery lines into a central vapor recovery system) and set points to be reached before shutdown, whereas a safety function system design would require 1 out of 6 set points reached to activate shutdown (thus the safeguard is not functional – unrevealed to operators and PHA team?).