ExxonMobil

Coke Drum MOV PLC Permissive Interlock System Availability

REFCOMM
MUMBAI
17-20 Oct 2016

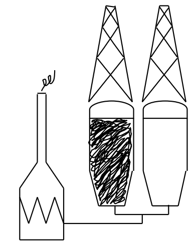
Energy lives here™

Presented by Mitch Moloney of **ExxonMobil Research & Engineering**

mitchell.j.moloney@exxonmobil.com

@ Mumbai   coking.com   October-2016

Coke Drum MOV PLC Permissive Interlock System Availability



Topics:

(1) Key Points Summary

(2) PLC interlocks History

(3) Probabilities and Risk

(4) Cyclic LOTO

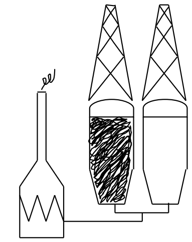
(5) PLC System Design

(6) Maintaining Operational Integrity

- Bypassing Procedures
- Safety Criticality and Control of Defeat
- Availability Tracking & Bad Actors
- MOV Inspection and PM
- Testing / Failure Modes

Special Thanks to **Sebastian Seider** for all his hard work that benefits our company and the industry !!

Coke Drum MOV PLC Permissive Interlock System Availability



Key Points:

Coker Structure Valve PLC Permissive Interlock Systems (PPIS's) are ***UNIQUE*** Safety Instrumented Systems (SIS's)

=> They are "active" NOT 'passive watchdog" systems

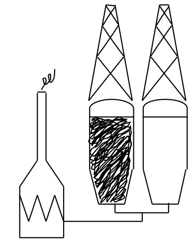
=> The entire coker SIS is safety critical

The Coker PPIS and back-up manual procedures (Control of Defeat) *together* must reduce the probability of incorrect valve line-up by two orders of magnitude (a factor of 0.01) versus a normal manual one-man procedure

=> The PLC system should be available from 90 to 99% of the required logic matrix line-up steps (95% recommended)

=> The CoD manual procedure must be effective at least 90% of the time

Coke Drum MOV PLC Permissive Interlock System Availability



Key Points (cont'd):

A proper Coker PPIS Inspection and Maintenance Program is required

=> Availability must be tracked and targeted as part of this program

Proper Lock-Out and Tag-Out of manual valves, De-Clutch Hand-Wheels and MOV's

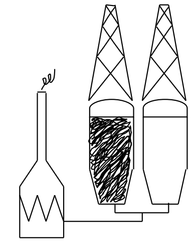
Testing requirements will be as follows:

=> Complete system testing (SAT equivalent) very TA

=> Any change to the logic matrix requires an SAT per MOC OIMS 6.3

=> System Use + Inspection & Repair programs meet passive SIS SIL test requirements

Coke Drum MOV PLC Permissive Interlock System Availability



Company History

1993, an operator was on the wrong drum pair and switched feed to an open drum, resulting in a fire and serious injury (this preceded a more serious fire in the same year)

=> Checklist, Lock-Out-Tag-Out (LOTO) and console radio confirmation was in place; the field operator (qualified, but < 2yr experience) verbally was on the correct drum, but actually on the wrong drum pair

As a result, refinery management decided to create automated valve operations with PLC logic-controlled oversight of all coke drum valve operations

=> The first system was started up 1995 as part of a coker rebuild project

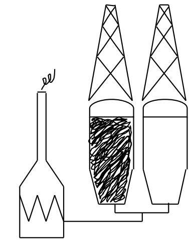
=> The 2 other site cokers received IL's by 1999

2001 - a 4^{th} largely-identical system was done as part of a grassroots coker project that started up in.

2004 - development/implementation of formal corporate-wide risk assessment process

=> The PLC Logic Matrix is an XOM-proprietary design

Coke Drum MOV PLC Permissive Interlock System Availability



Company History (cont'd)

2005 - ExxonMobil upgraded their Venezuelan Upgrader Coker with installation of the 5th PLC-based design and additional valve motor operators

=> Original 1998 design consisted of a simple hard-wired interlock between the feed inlet block valve and the utility header valve (drain, WU, steam, quench water)

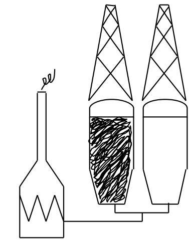
=> The system was justified based on improved reliability incentives since formal project safety risk assessment / justification techniques were not implemented

=> The PLC design and logic matrix were XOM-based analogous to previous designs

2007 - the Beaumont DCU implemented a complete Safety Upgrade Project

=> This was the first coker interlock system justified by formal safety risk assessment techniques

=> Project Scope – 6th Valve PLC Interlock System, Auto Top and Bottom Deheaders, Enclosed Cutting Shack, Structure Water Deluge



Company History (cont'd)

Following Beaumont's Risk Assessment, the other ExxonMobil DCU Structure Operations were formally risk assessed

=> Six sites; ten DCU's

2014 - The 7th PLC-based Valve Interlock System was installed on Chalmette No 2 Coker

=> Given the desire to minimize turnaround duration & project cost, all wiring was installed during unit operations and MOV's during annual pig decokes

=> This was the first project justified based on quantified risk reduction vs cost, to allow prioritization with other competing projects

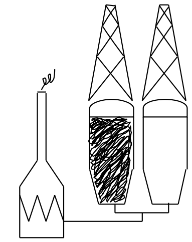
2015 - The 8th System for the Torrance North & South Cokers was completed

=> Early completion was possible due to FCC shutdown following an ESP Explosion

2016 - Joliet will be the 9th System installed

2017 - Antwerp will the 10th System

Coke Drum MOV PLC Permissive Interlock System Availability



Approximate Risk Probabilities in Play:

Creating an incorrect valve line-up (can be 2 valves) on the drum structure has a base probability of 0.001 (or 1 in a 1000 times)

MOV's with PLC Interlock lower the probability to 0.00001 (or 1 in 100,000 times), two orders of magnitude

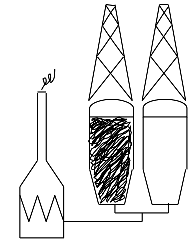
A well-controlled and stewarded LOTO program with well-trained and capable operations technicians lowers the probability to 0.0001, an order of magnitude

However, LOTO programs can fluctuate, and deteriorate, in effectiveness because ultimately they are administrative controls

Such controls rely on humans to always do the right things
=> be properly trained, have had enough sleep, not be distracted, not be bored by repetitive tasks, know how to deal with all equipment failures, have proper reinforcement on procedures, follow all procedures, not be rushed to meet cycle time deadlines, etc…)

For these reasons it is difficult to view *Cyclic LOTO* programs as permanent risk mitigation.

Coke Drum MOV PLC Permissive Interlock System Availability



Cyclic LOTO – Lock-Out, Tag-Out

The original goal of Lock-Out, Tag-Out (LOTO) was to prevent maintenance and contract workers from opening a valve that would send auto-ignitable hydrocarbon to an open coke drum

The use of LOTO was subsequently expanded to help reduce the risk that an operations technician would make a valve operations error.

Main Risks:

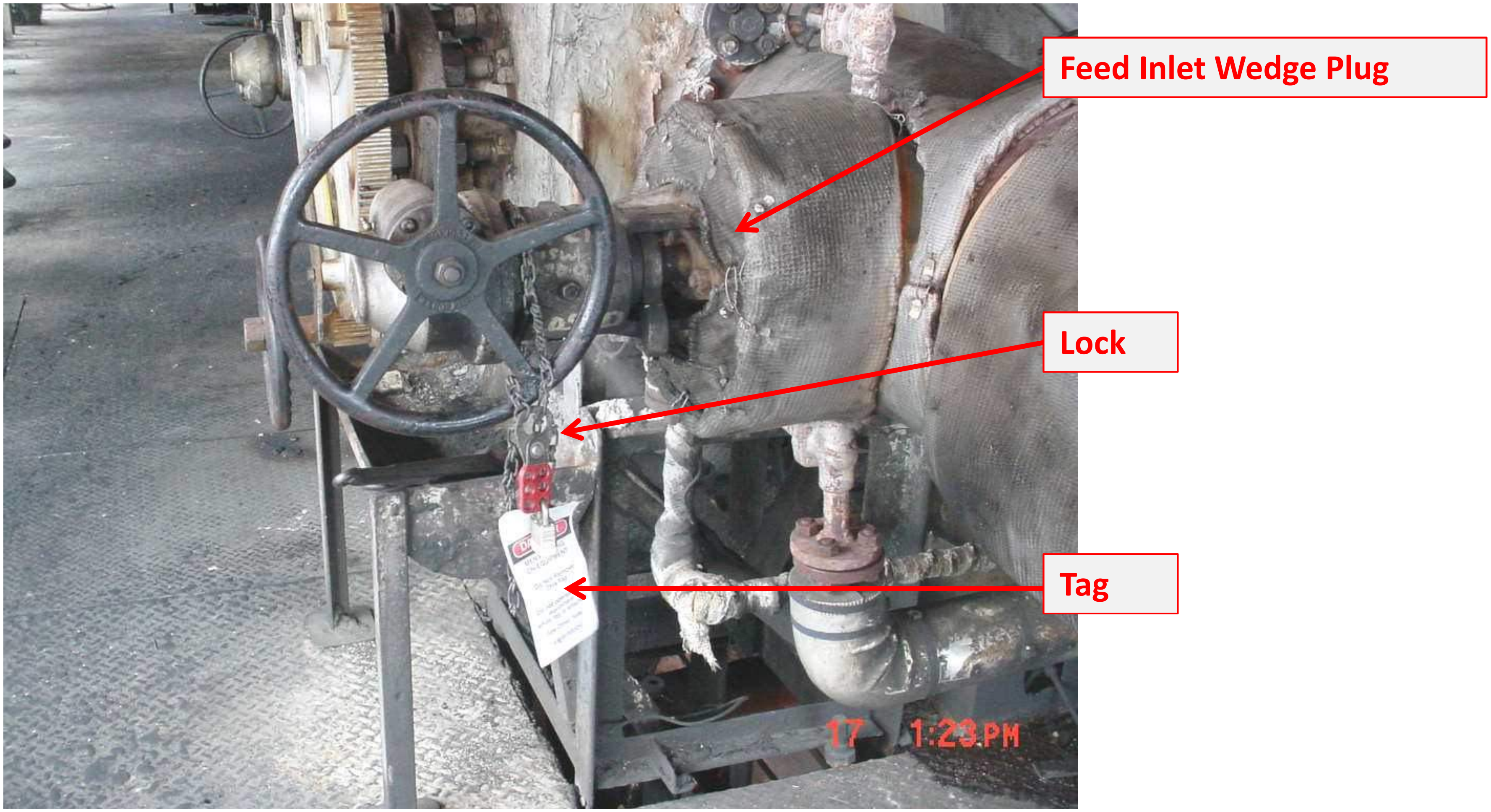
- Technician on wrong drum pair
- Technician omits a valve closure step
- Technician on wrong drum out of sequence

Features added (Enhanced LOTO):

- Paper checklist (has evolved to electronic via IntelaTrac)
- Enhanced Signage
- Dual Verification (2nd field technician and/or console supervisor)
- Frequent Training Refreshers
- Frequent Audits

Coke Drum MOV PLC Permissive Interlock System Availability

LOTO – Lock-Out, Tag-Out



Coke Drum MOV PLC Permissive Interlock System Availability

Advanced Cyclic LOTO – Lock-Out, Tag-Out

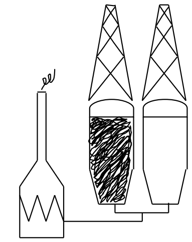
Locks and chains are placed on valves to prevent any other person from opening a valve by mistake and cause loss of containment. This applies to drums being decoked and drums in coking service.

Utilizes lock boxes, where each operator locks valves open or closed and places his key in a box. The locks can only be opened by obtaining the key in the lock box, which can be done using that operator's key or a master key ("Tech Lock") held by an Operations Supervisor.

Locks & Chains

Technician Lock Boxes

Coke Drum MOV PLC Permissive Interlock System Availability



PPIS Design Features

Valve Position Reliability

=> No external magnetic proximity switches

=> Valves are motor-operated with internal position switches

PLC Logic

=> The logic matrix relies on unique valve position relationships that must always be true; no sequencing of steps or process data input needed

=> Opening or closing a valve requires at least two other valve line-ups be validated by the PLC

System Design Basis Criteria

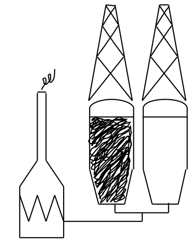
=> All components of the Structure Valve PLC Permissive Interlock System should result in a system availability of 90 to 99%

- Safety Criticality is applied to all components of the system
- Control of Defeat (Approval to Operate Escalates with Time) is applied to all components

=> When manual verification and movement of normally interlocked valves is required, that procedure requires dual verification of the proper valve line-up and communication with the Console when valves are being moved

- Position Switch or Relay failures require request of a permissive bypass
- Failure of the Motor will require use of the Declutch and HandWheel

Coke Drum MOV PLC Permissive Interlock System Availability



Maintaining Operational Integrity of the DCU PPIS

The key features of an effective strategy are:

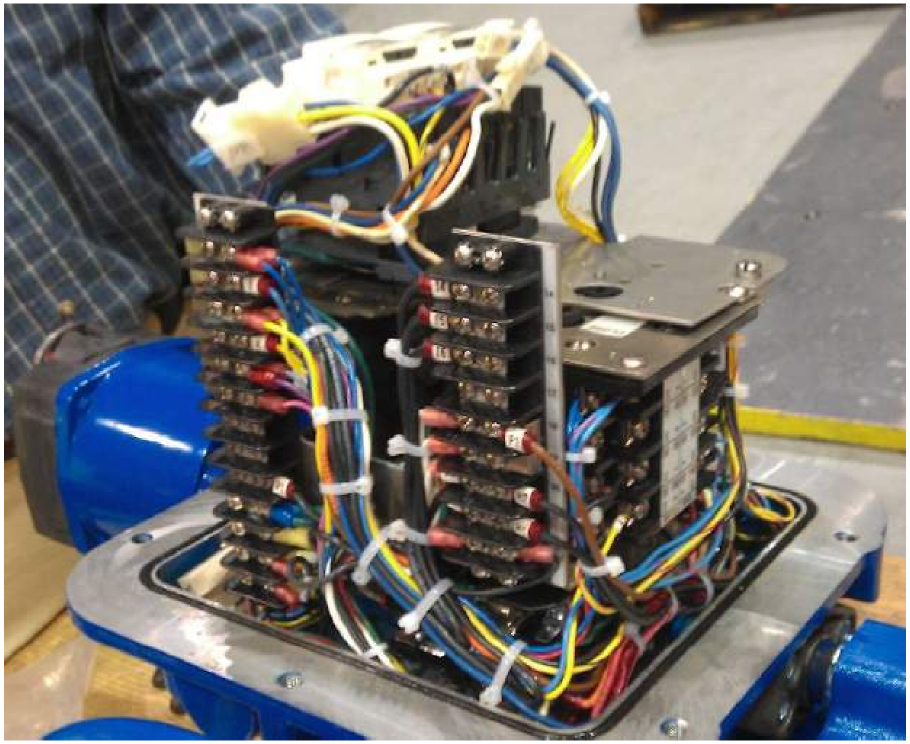
- A Control of Defeat (COD) work process and formal guidelines for use of bypass functionality
- Availability Tracking (explained below)
- Bad actor monitoring and continuous improvement
- Valve/actuator preventative maintenance (PM) program (service factor considerations)
- Proper Electrical interface design characteristics
- A proper testing strategy (for each component and combined system)

The central recommendation is to classify all components of the interlock system (as required for full functionality) as Safety Critical.

Coke Drum MOV PLC Permissive Interlock System Availability

PPIS Bypass Procedure Recommendations

The recommended electrical interface design should be such that the PLC locks out motive power to the motor actuator, while allowing signal indication



BYPASS FUNCTIONALITY

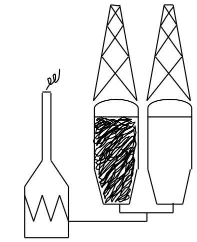
Below is an overview of interlock bypass capability and recommended COD practices:

Limit switch bypass (allow the drum sequence to proceed where a failed limit switch would inhibit a required valve movement; i.e. bypass the output loop of the valve in question to allow other valves to be moved (resets after 5 mins).

Valve (Maintenance) Bypass: Inhibit the valve's interlock for maintenance purposes such that it can be operated freely, i.e. bypass the input loop to the valve in question. No automatic reset. COD in place.

Drum bypass: Inhibits interlock for maintenance for all valves on the drum pair. No automatic reset. COD in place.

Coke Drum MOV PLC Permissive Interlock System Availability



Maintaining Operational Integrity of the DCU PPIS

Safety Criticality Applied to Operational Oversight

=> This designation provides immediate ‘break-in’ repair

=> Availability must be tracked and stewarded (Example Calculation on next 2 slides)

Control of Defeat Procedures

=> “Any deactivation or non-standard operation of safety critical equipment or systems must be documented and approved …“

=> First signature approvals are Area Operations Lead and Shift Supervisor

=> If the deviation lasts more than 24 - 72 hrs, signature must be obtained from the next highest management level, continually progressing with time.

=> Only one CoD is required following failure of a specific component, even though a permissive bypass may be required several times prior to repair of the failed component.

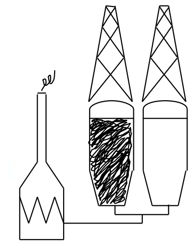
DCS Valve Bypass Monitoring (to highlight bad actors)

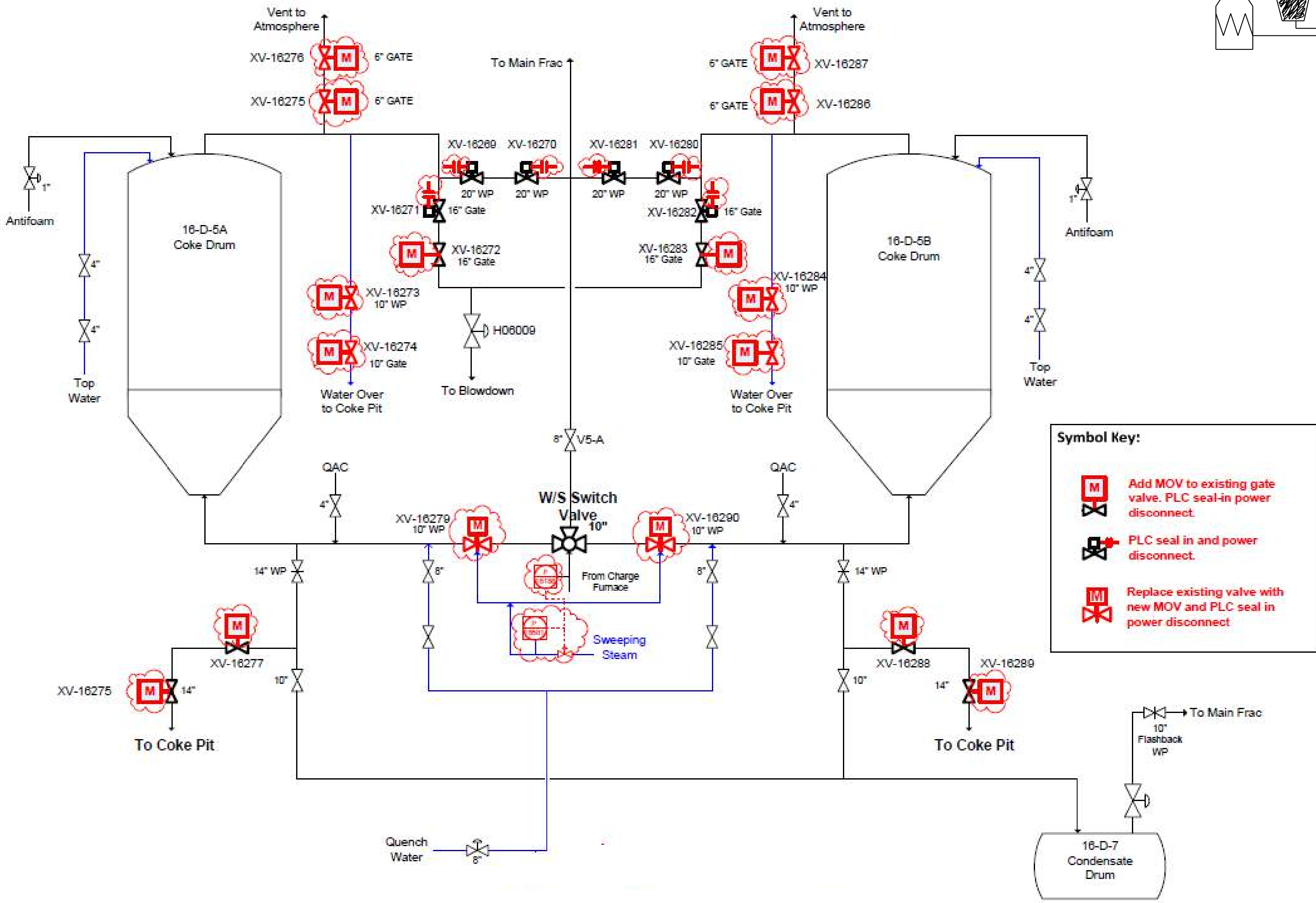
=> PLC oversight of individual valves can be bypassed with automatic reset after 5 minutes (due to various failures of the MOV, typically limit switches, relays or circuits)

=> DCS Program counts the bypasses and displays on Interlock Master Screen

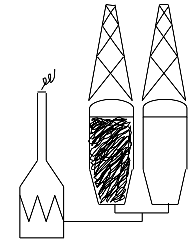
ExxonMobil

Coke Drum MOV Layout Example

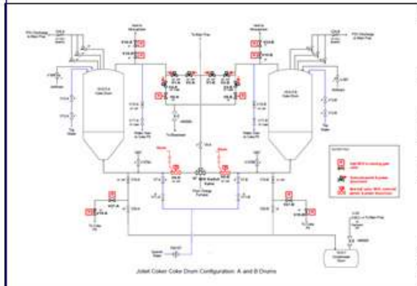




Coke Drum MOV PLC Permissive Interlock System Availability

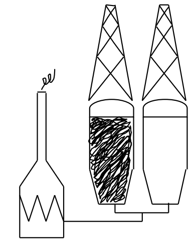


The PLC Matrix (Basis for Example Calculation)

		Feed / Switch Valves		Fractionator Valves		Blowdown Valves		Drain Valves		Vent Valves	
	Drum	A & B	A	A	A	A	A	A	A	A	A
	Valve Name	Wilson-Snyder Switch Valve	Feed Isolation Valve	Vapor Valve to Fractionator (upstream)	Vapor Valve to Fractionator (downstream)	Vapor Blowdown Valve (upstream)	Vapor Blowdown Valve (downstream)	Water Drain to Coke Pit (upstream)	Water Drain to Coke Pit (downstream)	Vent to Athmosphere (upstream)	Vent to Athmosphere (downstream)
	Valve Type (existing)	W/S	Wedge Plug	Wedge Plug w/ MOV	Wedge Plug w/ MOV	Gate W/ MOV	Gate	Gate	Gate	Gate	Gate
	Valve Size	10"	10"	20"	20"	16"	16"	14"	14"	6"	6"
	Valve Type (new)	W/S	Ball Valve w/ MOV	Wedge Plug w/ MOV	Wedge Plug w/ MOV	Gate W/ MOV	Gate W/ MOV	Gate W/ MOV	Gate W/ MOV	Gate W/ MOV	Gate W/ MOV
	Scope of Work	N/A	New ball valve with interlocked MOV	Add solenoid cutout to existing MOV	Add solenoid cutout to existing MOV	Add solenoid cutout to existing MOV	Retrofit with MOV actuator & interlock relay	Retrofit with MOV actuator & interlock relay	Retrofit with MOV actuator & interlock relay	Retrofit with MOV actuator & interlock relay	Retrofit with MOV actuator & interlock relay
	Valve Number	WS-X	V6-X	V1-X	V2-X	V4-X	V8-X	V27-X	V19-X	V15-X	V14-X
	Proposed Interlock Level	N/A	Interlocked	Interlocked	Interlocked	Interlocked	Interlocked	Interlocked	Interlocked	Interlocked	Interlocked
ACTION	VALVES	PERMISSIVES									
1) Drum A Coking, Drum B on Heatup - Valve Starting Position		A	O	O	O	C	C	C	C	C	C
2) Close Condensate to blowdown on B	V18-B										
3) Open oil inlet insolation valve on B	V6-B										
4) Switch the Wilson-Snyder valve to B	WS-B										
5) Close oil inlet valve on A	V6-A										
6) Open B/D valves on on A	V8-A/V4-A		C					C	C	C	C
7) Close vapor valve to frac tower on A	V1-A/V2-A		C			NC	O				
8) Close antifoam	V-097										
9) Close B/D valves on A	V8-A/V4-A										
10) Open water-over valves	V16-A/V17-A										
11) Open first and second top vent to atmos on A	V15-A/V14-A		C	C	C	C	C				
12) Open first and second drain valve to pit on A	V19-A/V27-A		C	C	C	C	C				
13) Unhead / Cut / Rehead											
14) Close first and second drain valve to pit on A	V19-A/V27-A										
15) Close first and second top vent to atmos on A	V15-A/V14-A										
16) Air free and pressure test											
17) Open drain valves and depressure	V19-A/V27-A		C	C	C	C	C				
18) Close drain valves	V19-A/V27-A										
19) Open Condensate valves on A (NOT INTERLOCKED)	V18-A/V20-A		C					C	C	C	C
20) Open drum ovhd valves to frac tower on A	V1-A/V2-A					C	C	C	C	C	C
21) Close condensate to blowdown valves on A	V18-A/V20-A										
22) Open oil inlet valve on A	V6-A			O	O	C	C	C	C	C	C

NOTES:
"C" Means the Valve Needs to be CLOSED to perfom the specified valve movement for that row.
"O" Means the valve needs to be OPEN to perform the specified valve movement for that row.
"NC" Means the valve needs to be NOT CLOSED to perform the specified valve movement for that row.

Coke Drum MOV PLC Permissive Interlock System Availability



The PLC Matrix (Basis for Example Calculation)

Any time manual verification and movement of normally interlocked valves is required, that should be recorded as an "Unavailability Unit". This can be required by failure of a limit switch, a relay, a wire in the motor actuator, etc.

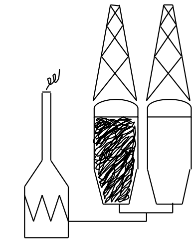
=> By exception, failure of a valve, requiring leaving it in the open position and use of a special single block operation, shall be not be included in the availability calculation, being a special, infrequent case

EXAMPLE:

The following malfunctions occur during a 1 year of operation for a drum pair (700 drums):

- The vent valve limit switch is broken during 4 drum cycles and then 3 drum cycles. This results in bypassing the interlock system for 3 steps on each of these drum cycles. The 5 remaining steps are still protected.
- The feed inlet valve limit switch is broken for 2 drum cycles. This will result in bypassing the interlock system for 4 steps on each of these drums. The 4 remaining steps are still protected.
- In these two instances, 29 bypasses are required. During the year, 131 other bypasses were required, yielding a total of 160.
- The total annual number of PLC matrix steps is 700*8=5600.
- The overall annual availability would be (5600-160)/5600 = 97.1%

Coke Drum MOV PLC Permissive Interlock System Availability

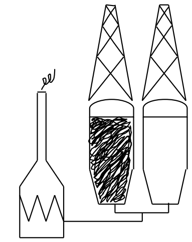


Maintaining Operational Integrity of the DCU PPIS

- At a minimum, annual PMs conducted for valves and actuators. Higher frequency may be justified for valves related to loss of containment scenarios and operating experience.
- Scope of PM's covering all key focus areas (categories shown on diagram to the right)
- Quarterly STM purge flow verification
- Quarterly Amp monitoring and trending over time (optimally via. Intelatrac rounds)
- Over-torque protection for manual operation
- Actuator spring strategy
- Valve condition monitoring program

VALVE AND ACTUATOR INSPECTION FOCUS AREAS
External Visual Inspection (fasteners, grease, conduit, etc.)
Valve Stem, Protector, Stem Nut
Insulation
Internal Visual Inspection (lid seals, pinched wires, grease, etc.)
Lubrication
MDPI Gear Train
Limit Switches
Control Station
Torque Switches
Electrical Control Components (heater, wiring, contactor, etc.)
De-Clutch operation
Motor Test
Valve Stroke Times
Valve Opening/Closing Amps
STM Purge checks

Coke Drum MOV PLC Permissive Interlock System Availability

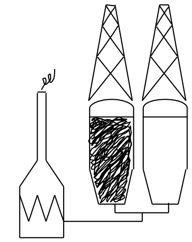


Maintaining Operational Integrity of the DCU PPIS

An effective site PM program is critical to maintaining reliability of MOV's and preventing significant loss of system availability. Common Issues:

- Incomplete PM's with no "As Found / As Left" documentation
- Findings are not shared with process owners as required to drive proactive follow-up.
- No formal work process to ensure findings incorporated into maintenance work lists.
- Information and results are not historized and monitored.
- Steam Purge verification and Torque / amp monitoring rounds are not conducted.
- Interlocked systems are not maintained/tested per safety guidelines

Coke Drum MOV PLC Permissive Interlock System Availability

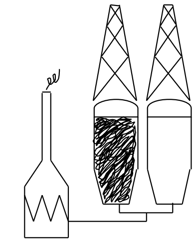


Maintaining Operational Integrity of the DCU PPIS

The most common failure mechanisms include:

- Fouled valve internals (may be due to loss of or inadequate steam purge)
- Broken actuator components (limit switches, contactors, wet components)
- Manual over-torqueing or incorrect setting on torque switches
- Installation deficiencies
- Vibration-related issues (such as contactor bounce, loose wiring, etc.)
- Maintenance/Lubrication deficiencies
- Design mis-match of valve/actuator/gear

Coke Drum MOV PLC Permissive Interlock System Availability

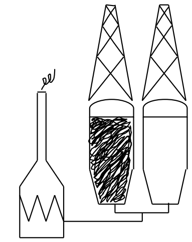


Maintaining Operational Integrity of the DCU PPIS - TESTING

- It is recommended to NOT apply classic SIS component analysis to meet SIL requirements.
  - The system operates on an integrated basis & should be viewed holistically
  - The vast majority of failures are found through use of the system

TEST TYPE	FREQUENCY	SCOPE
Pre-startup acceptance test	One Time	Initial acceptance testing to ensure logic integrity and confirm all components of the system are functioning as expected
MOC-driven testing	As Needed	Testing driven by any post-startup changes to PLC logic or other high risk components of the system (scope set by site MOC process)
Rigorous downtime testing	Approx 5 yr.	Testing strategy involves placing a demand on the system to open each valve that is considered a release point and determining if proper action was performed
PM inspection	Approx 1 yr.	Inspection conducted as part of valve PMs focusing on any deteriorating components of the actuator (seal wear, loose wiring, etc)

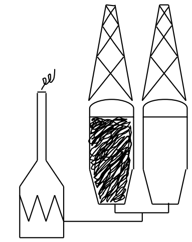
Coke Drum MOV PLC Permissive Interlock System Availability



Maintaining Operational Integrity of the DCU PPIS
– FAILURE MODES

Component	Issue	Event Sequence/Mitigation	Testing
PLC Logic	Triconex logic error giving permissive to open a valve while unsafe	Failure does not directly lead to consequence (procedural mitigations in place).	Initial acceptance testing would ensure logic integrity if access to Triconex logic is restricted. MOC procedures would drive testing if any changes to logic were made.
Open Limit Switches	Faulty limit switch allowing unsafe valve movement on another valve	Issue with limit switches would be detected on previous drum cycle when valve movement is performed.	Tested as part of normal operation.
Closed Limit Switches	Faulty limit switch allowing unsafe valve movement on another valve	Issue with limit switches would be detected on previous drum cycle when valve movement is performed.	Higher risk than open limit switches since closed limit switches are associated with confirming isolation from live process. Tested as part of normal operation.
Seal-in contactor bounce	Seal-in contactor bouncing due to vibration and sealing itself-in resulting in valve movement	Mitigated in recommended design. Sites with exposure deenergize valves when not in use.	The recommended design relies on Triconex to complete the control circuit and maintain valve movement. An alternative design utilizes a series of orthogonal contactors to prevent sealing in circuit due to vibration. Testing would not provide incremental benefit as action occurs on failure.
Reversing contactor becoming stuck	Reversing contactor getting stuck due to vibration/damage	Movement would follow the commanded action and the valve would remain there and not work until repaired.	Highly unlikely due to robust design and no history at sites. Testing would not provide incremental benefit as failure would occur on initiation and either work or not.

Coke Drum MOV PLC Permissive Interlock System Availability



Maintaining Operational Integrity of the DCU PPIS

– FAILURE MODES (cont'd)

Component	Issue	Event Sequence/Mitigation	Testing
Solid state PLC relays	Stuck Triconex relays failing in a mode that completes the circuit	Failure does not directly lead to consequence (procedural mitigations in place).	This low probability failure would be detectible through SDO (supervised discrete output) diagnostic alarm.
Actuator electrical components	Water/coke causes short circuiting resulting in valve movement	This failure would most likely cause loss of power via overcurrent or ground fault.	Regular valve PMs would ensure that actuator housing seal is in good condition and water does not collect inside housing.
Loose wiring	Loose wiring causes short circuiting resulting in valve movement or bypassing PLC oversight	Would most likely result in inoperability	Could be caused by vibration or heat. Regular valve PMs would ensure that there are no loose wires inside actuator housing.
Actuator wiring issue (such as jumper bypassing interlock validation)	Jumper installed across section of circuit which is completed when PLC validated	Failure does not directly lead to consequence (procedural mitigations in place).	This type of failure would not be detected during normal operation and is one of the drivers for rigorous downtime testing.
Broken push button	Push-button stuck in the closed position.	PLC oversight in place mitigating scenario.	Valve would move immediately upon receiving permissive but the PLC oversight would still be in place preventing any unsafe movements

ExxonMobil