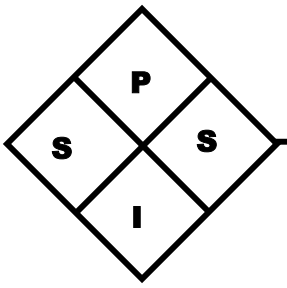


SafePlex Systems, Inc.

PARTIAL STROKE TESTING COMPARISON PAPER

- ***SafePlex SILstroke-3***
- **ASCO 2oo2D**
- **Emerson DVC6000**

The evaluation provided is based on the best known information in the public sector. SafePlex Systems provides this comparison for the general usage of the reader, and not as a final and definitive evaluation.

COURTESY OF SAFEPLEX, INC.

Specializing in Systems for Safety and Critical Control

ANSI/ISA S84.00.01-2004

During the year 2004 ANSI/ISA S84-1996 was replace with the contents of IEC 61511, and is now known as ANSI/ISA S84.00.01-2004. Added to the IEC 61511 was one grandfathering paragraph, investing ESD systems designed under ANSI/ISA S84-1996.

This paper points out one of the major differences between S84-1996 and S84-2004. That is - the requirement for Hardware Fault Tolerance (HFT). Hardware Fault Tolerance is different from Fault Tolerance (FT). HFT is defining a serial relationship such as 1oo2 or 1oo3 whereas FT is defining a parallel relationship between devices such as 2oo2 or 2oo3.

Because of the HFT requirements within the S84-2004 for SIL 2 and SIL 3 loops, a SIL 3 certificated device under IEC61508 may not meet the HFT requirements within S84-2004.

In paragraph 11.4 of the S84-2004 resides the HFT table. The base case for field devices used in a SIL 2 safety loop (SIF), a HFT of one (1) has to be applied (1oo2). The base case for field devices used in a SIL 3 SIF, a HFT of two (2) has to be applied (1oo3). If the device(s) being used has >50% known failure mode, then the HFT can be lower by one (1), meaning the SIL 2 SIF would have a HFT=0 and SIL 3 SIF would have a HFT=1.

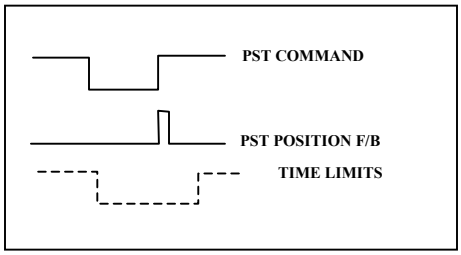
This above paragraph has two imbedded conclusions:

1) To avoid needing two ESD valves for a SIL 2 SIF, the owner has to use partial stroke testing (PST). Otherwise the ESD valve known failure mode will be <50%, making the second valve necessary to meet the HFT table minimum limits.
2) A SIL 3 loop will require two ESD valves with PST just to avoid requiring three ESD valves (1oo3).

Partial stroke testing will provide diagnostic coverage factor of approximately 70 to 80%. The exact number is hard to define because of the application's definition of tight shutoff, how much solids within the fluids, etc. However, the PST will meet the >50% known failure mode requirement for the S84.00.01-2004 Part 1 Clause 11.4.

SILstroke-3

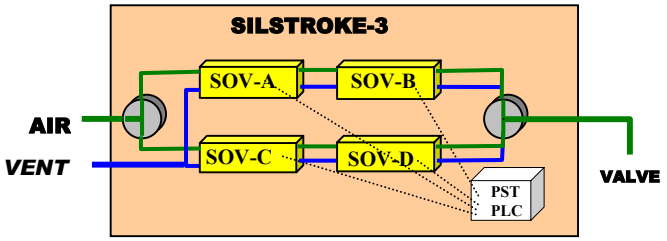
The SafePlex Systems' SILstroke-3 architecture is based on two-out-of-four (2oo4) solenoids with an on-board PLC for performing the PST testing of the ESD valve and the full stroke testing of the four (4) SOVs --- all ESD logic is performed by the ESD system --- all PST logic is in the on-board PLC. The 2oo4 solenoids consist two sets of parallel 1oo2 solenoids *(HFT=1)*. The parallel relationship creates ***fault tolerance*** in case one SOV fails close. The series relationship (1oo2) creates ***Hardware Fault Tolerance of 1*** in case one SOV fails open. By-passing of the a failed SOV occurs in 1oo2 pairs – leaving the other 1oo2 SOV pair in control of the ESD valve.



SILstroke-3 has a TUV SIL 3 certification based on the IEC 61508 product standard. Though certified under the IEC 61508, SILstoke-3 was design using the techniques of DIN19250. DIN19250 design standard requires statistical availability, plus diagnostic coverage and mitigation of dangerous failure(s) to be SIL 3 rated. This DIN 19250 design exceeds the design requirements of ANSI/ISA S84.00.01-2004 standard. The S84-2004 only requires a HFT=1 for SIL 3 safety loops (SIFs), meaning one set of 1oo2 SOVs with a 51% or greater safe failure fraction (SFF). That is why SILstroke's SOVs are in a 1oo2 series arrangements with a pressure switch mounted in each SOV to verify and validate its operations. These pressure switches are monitored by the on-board PLC as part of the diagnostic coverage.

FULLY FAULT TOLERANT – FAILSAFE – 100% DIAGNOSTIC COVERAGE

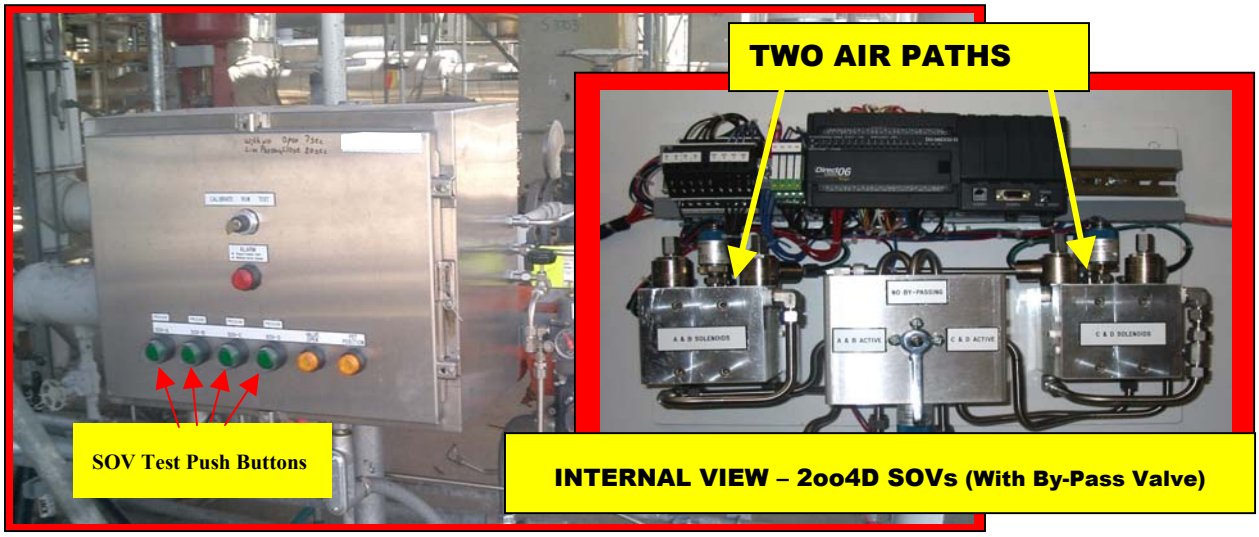
The SILstroke-3 PST sequence consist of the full stroke testing of each SOV *(individually)* and then the PST of the ESD valve. Programmed into the on-board PLC is a reasonability time override in case the PST feedback does not occur within a defined period of time.



SCOPE OF CERTIFICATION

SILstroke-3 scope of certification is a complete PST system, excluding the ESD valve. There are no major parts of the SILstroke-3 PST system that is outside of the scope of certification. Within the on-board PLC is the ability to trigger the PST based on time, local command, and remote command. The calibration of the SILstroke-3 box is completed by the local keyswitch. The timing factors are adjusted automatically by the on-board PLC based on the speed of each valve. The max / min limits are adjustable via scaling factors.

SILstroke-3 Summary



SILstroke-3 Features

1) The architecture of SILstroke is 2oo4D. It is both fault tolerant and fail safe.

No single solenoid failure will prevent this device from operating safely, or cause a spurious trip.

2) All solenoids are tested prior to a PST, and the PST is cancelled and alarmed should any SOV test fail.

No calibration or PST cannot over-stroke the valve or cause a spurious trip.

3) Two limit switches are typically used to provide movement and position feedback.

Analog signals can be supported as well.

4) The SILstroke device is not installed on the valve like a positioner.

It replaces the existing SOV.

Can be up to 30 feet away from the ESD valve-those hard to reach valves

5) No PES (logic solver) programming or hardware changes are required to support SILstroke.

Independent logic for the PST

PST PLC is non-interfering in solenoid operations

6) Any solenoid can be by-passed and replaced on line, without degrading the safety function.

The maintenance by-pass valve only by-passes one set of SOVs - the other set controls the ESD valve

7) A PST can be initiated by the SIS, automatically at a periodic interval, or manually.

Local testing can be of the SOVs only or the ESD valve

8) SILstroke is calibrated in place under actual process operating conditions.

A PC is not required for calibration.

9) The solenoids provides high Cv, and can be used with larger valves.

Each SOV path through the SILstroke-3 box is 1.7Cv rated (80 cfpm at 80 psig to atmosphere)

10) PST status (history and alarms) is available using MODBUS, MODBUS TCP, or OPC.

Provides diagnostic and testing history

11) The device is simple to install, calibrate, operate and maintain.

The device is FM Class I, Div. 2 rated, and requires less that 500 ma. to operate.

12) The device is TUV approved to SIL 3 per IEC 61508, and the design is patented.

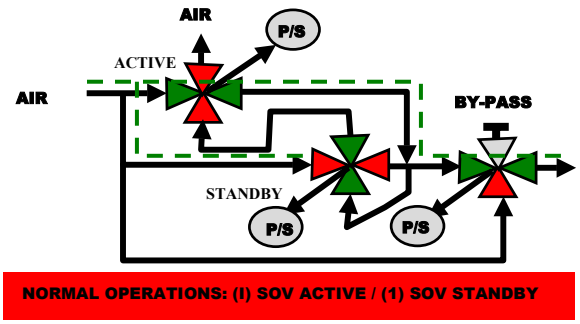
Has a HFT of one (1) - Meeting the Field Device HFT Table within IEC 61511

13) SILstroke can be used with Air-to-Open (Spring return), Air-to-Close (Spring return), or Dual Action Valves.

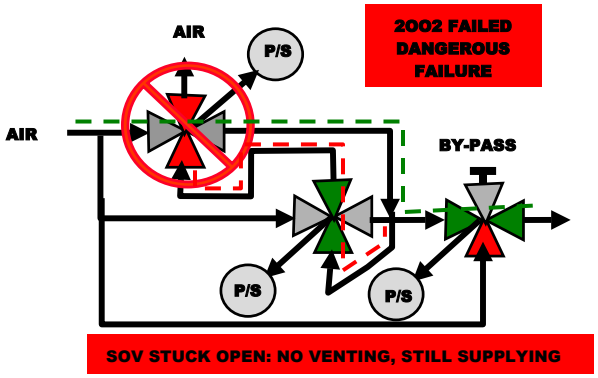
SILstroke is the most comprehensive, cost effective PST solution available.

ASCO RSC-2oo2D OVERVIEW PAPER

The ASCO Partial Stroke Testing box air supply to the ESD valve's diaphragm is based on a dual two-out-of-two (2oo2) solenoid arrangement, and the ESD valve's venting is based on a 1oo2 arrangement. This means either of the 2oo2 solenoids can supply air to the diaphragm of the ESD valve, and both solenoids have to be closed (1oo2) to vent the air from the ESD valve's diaphragm. Each solenoid (SOV) is equipped with a pressure switch to verify SOV open/close status, and spool movement.



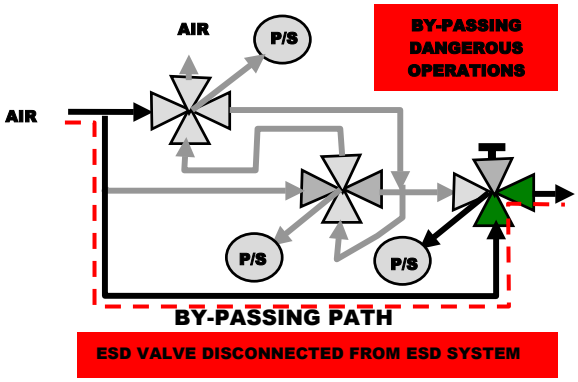
The ASCO SIL 3 certificate is a "type" certification. This means the certificate verifies that "statistically" the safety performance of the ASCO 2oo2D box falls into the SIL 3 (10^{-3} to 10^{-4} PFD) range. The issue is, "statistical" availability is not equivalent to "safety" availability. Missing from the ASCO 2oo2D design is mitigation of dangerous failures, a critical aspect of "safety" availability. Per the ASCO TUV report, the dangerous failure content of the 2oo2 arrangement without mitigation is so high that only one SOV can be energized at a time, the other SOV must be in standby mode. ASCO states that all dangerous failures are detected by ASCO diagnostic, but fails to state that all dangerous failures are mitigated.



DANGEROUS FAILURE MODES

Stuck Open SOV

The 2oo2 is the most dangerous solenoid arrangement for a de-energize to trip designed ESD system. Adding a general purpose PLC to test the 2oo2 arranged solenoids, does not reduce the dangerous failure content. If either solenoid fails in a "stuck open position" the ESD valve will be held open. The testing PLC will inform the operator(s) of the stuck open solenoid failure, but the RSC-2oo2D cannot mitigate this dangerous failure. Therefore, the RSC-2oo2D is not hardware fault tolerant and does not have a *secondary means of de-energization (venting)*.

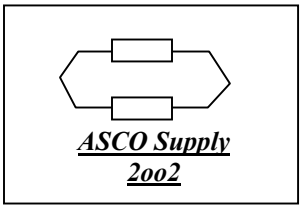


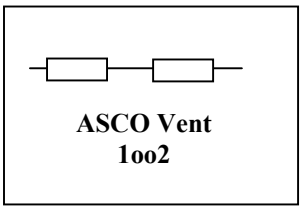
By-Passing

By-passing in the ASCO 2oo2D box disconnects the ESD valve from the ESD system. In the by-pass mode the ASCO 2oo2D box routes the air supply directly to the ESD valve's diaphragm. This allows the RSC-2oo2D solenoids to be removed. However --- an operator would have to manually close the ESD valve during maintenance by-pass if a trip should occur.

ASCO Summary

So in general the ASCO 2oo2D issues are:





1) The SIL 3 certification is based on "statistical" availability, not "safety" availability --- meaning that under lab conditions it is able to perform in a 10^{-3} to 10^{-4} PFD range.

2) The ASCO 2oo2 arrangement cannot mitigate the stuck-open solenoid failure, resulting in a dangerous failure mode.

3) ASCO maintenance by-pass valve can only by-pass both solenoid valves, and therefore the ESD system does not control the ESD valve while the ASCO by-pass is active.

4) The TUV report limits the ASCO 2oo2D box to a single solenoid (1oo1) operation with the second solenoid demoted to hot standby.

5) Both solenoids have to be in the closed position before the ESD valve's diaphragm can vent.

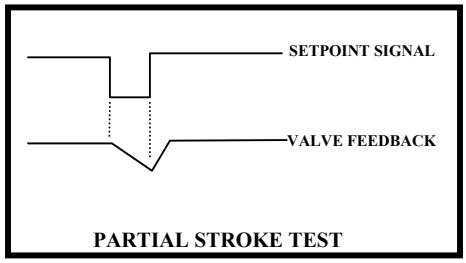
6) The VG800B design does not meet the HFT of one (1) and therefore does not meet the ANSI/ISA S84.00.01-2004 ESD SIL 3 safety loop (SIF) design standard. *See ANSI/ISA S84 – 2004 Part 1, Clause 11.4*

7) The ASCO package cannot test the solenoid(s) before PSTing the ESD valve. Failure to re-energize the active solenoid will over-stroke the ESD valve before the second SOV can be activated by the ESD system.

8) Cv rating is <1.0 – meaning longer ESD valve closure time. Quick exhaust valves are required for larger valves with short Process Safety Time factors.

EMERSON DVC6000 ESD "PST" APPROACH

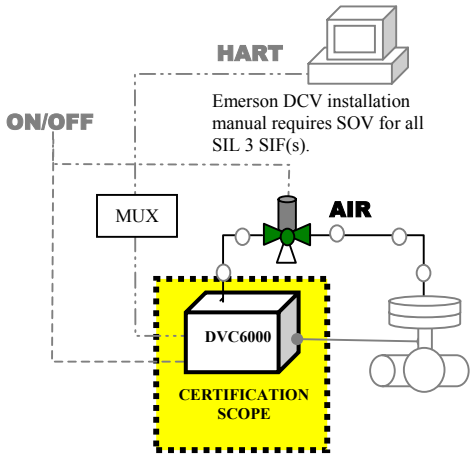
The positioner based PST approach is a proportional control style of valve movement. The movement is created by the ESD system step changing the positioner's set point value to the PST target value. The positioner monitors the speed of response, the quality of the response, and actual valve position. If the valve does not response within reasonable period of time, the positioner's microprocessor cancels the test.



The DVC6000 positioner has a TUV SIL 3 "type" certification based on the IEC 61508 standard. This means that its ***"statistical"*** availability falls into the SIL 3 range. Different from the DIN 19250 standard that requires statistical availability, plus diagnostic coverage and mitigation of dangerous failure(s) to be SIL 3 rated --- the IEC 61508 only requires statistical availability to qualify as SIL 3. This difference can mislead the end user into thinking that an IEC 61508 SIL 3 rating is equal to the DIN 19250 definition of SIL 3 and/or to the SIL 3 rating within IEC 61511 --- it is not the same safety rating.

DANGER: The DVC6000 is not "fail safe" or "fault tolerant."

The SIL 3 rated DVC6000 positioner used in ESD applications, is the same design as the general-purpose positioner used for control valves. No additional skills or mitigating hardware was included in the DVC6000 ESD version. Therefore the dangerous failures within the standard positioner still exist with the DVC6000 ESD version used on ESD valves.



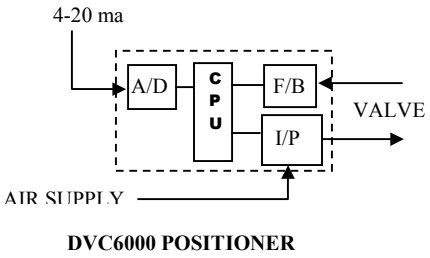
<u>The scope of the DVC6000 certification was limited to the pneumatic portion of the positioner only</u>. The electronics are considered to be non-interfering by using an OFF/ON signal to power the positioner. By doing this the Safety Failure Fraction (SFF) percentage was increased high enough to reach SIL 3. Other items outside of the certification are the – solenoid valve, and the PC with the ValveLink monitoring software. Yet without those uncertified items, the DVC6000 has little value as a PST system. When the DVC6000 is in series with these uncertified items *(i. e., the solenoid),* its SIL 3 rating is negated. When items making the safety loop are in series, the dangerous failure rate of each item has to be combined. This summation becomes the dangerous failure rate for the assembly. Therefore, if one of the items is SIL 1, the maximum rating for the assembly is SIL 1. I must conclude that this math result is the reason why Emerson does not openly discuss the need for the interposing solenoid. See below.

Positioner (SIL 3) + an ESD Valve *with PST testing* (SIL 2) + an untested SOV (SIL 1) = Rating (SIL 1)

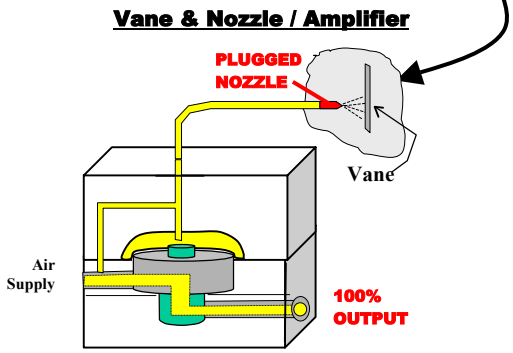
Furthermore, if the installation has two or more DVC6000 positioners, additional uncertified hardware is required to multiplex the HART signals to the PC based ValveLink software. First installation of the DVC6000 system could cost $10,000, and then add the cost of each DVC6000 at approximately $4,000.

DVC6000 Summary

So in general the DVC6000 issues are:



DVC6000 POSITIONER



1) The SIL 3 certification is based on "statistical" availability, not "safety" availability --- *the DVC6000 "positioner" FMEA SIL 3 evaluation was performed by "Emerson, not the TUV."*

2) Because the DVC6000 is not fail safe, it needs a solenoid as a *secondary means of de-energization* to:

   a) Negate I/P failures that could cause the "positioner" to be stuck at 100% output.

   b) To meet the HFT of one (1) as stated in ANSI/ISA 61511. *See ANSI/ISA S84 – 2004 Part 1, Clause 11.4.*

3) DVC6000 is not fault tolerant in design and does not support on-line repair.

4) DVC6000 partial stroke testing of the ESD valve does not test the solenoid, which is the *secondary means of de-energization*.

5) Most of the required valve monitoring system is not SIL 3 certified.

6) The TUV certificate is based on the DVC 6000 operating off of a digital output value, not an analog output value. This means that the HART signal is lost during valve closures.

7) Because the I/P is only partially bleed down enough to reach the 90% closure, the positioner is not tested for its ability to close the ESD valve --- only partially tested, like the ESD valve.

8) The venting rate of the positioner <20scfm – meaning that quick exhaust devices have to be used to vent larger valves within the SIF's process safety time.

9) The positioner must be mounted on the valve – meaning that hard to reach valves are very difficult to service.