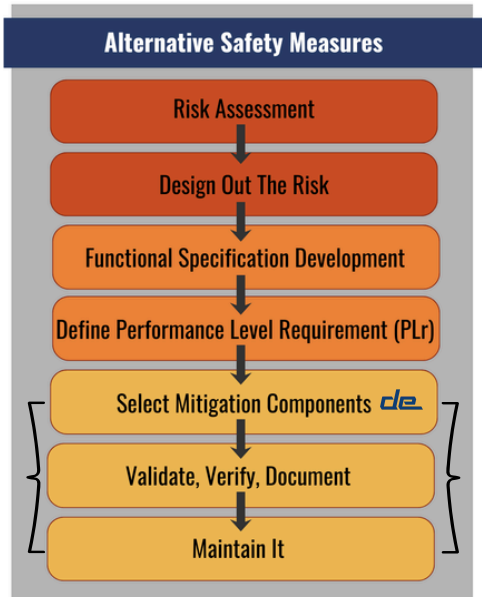
Build It. Prove It. Keep It.

How to select the right components, validate your safety system, and make sure it stays that way.

Over the past three months, we have covered Risk Assessment, Designing Out the Risk, Functional Specification Development, and Performance Level Requirement (PLr), the groundwork that must be in place before a single component is chosen. This month, we finish the process with the **final three steps**: ***Select Mitigation Components***, ***Validate, Verify, & Document***, and ***Maintain It.***



But first, the most common question we hear at this stage:

"What safety component should I buy?"

The problem is that machine safety doesn't start with components. It starts with understanding risk. A light curtain isn't automatically safe. A safety-rated valve isn't automatically safe. Even a device rated for PLe or SIL 3 doesn't automatically give the machine that same rating.

The complete safety function, from detecting the hazard through controlling the hazardous motion or energy, must be designed, integrated, verified, and validated as a system. **That is the difference between installing safety products and building a machine safety system.**

PART 1

Select Mitigation Components

Once you know the required safety function and its PLr, component selection becomes an objective exercise. The question shifts from: "*What should I buy?*" to "*What combination of components will meet or exceed the PLr I have defined?*" **That shift from product selection to system design is what separates a real safety system from a collection of safety-rated hardware.**

The Three Building Blocks of Every Safety Function

A complete safety function is typically a system of three elements. No single device is a safety function on its own, the input, logic, and output must all be specified, rated, and validated together:

Input Device

Triggers the safety function

Examples

- Guard door switch
- E-stop
- Light curtain
- Pressure sensor

Logic Device

Monitors input, controls output, detects faults

Examples

- Safety relay
- Safety PLC
- Safety controller

Output Device

Executes the safe state when commanded

Examples

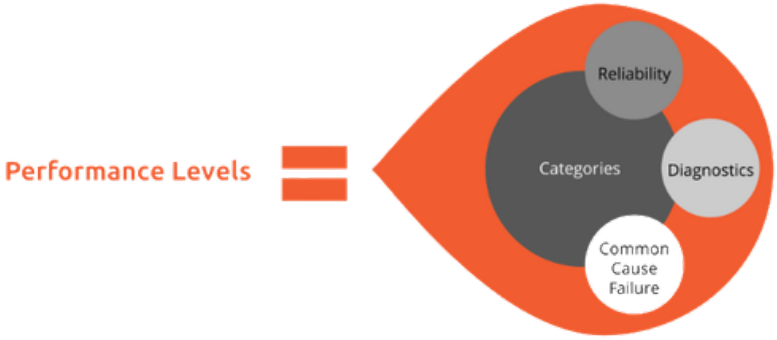
- Safety valve
- Rod lock
- Load-holding valve

The logic device is where most of the intelligence lives. It does not simply pass a signal, it monitors the input device continuously, commands the output device, reads feedback signals to confirm the safe state was actually achieved, and holds the machine in a faulted state if something does not check out.

A safety relay does this with hardwired logic; a safety PLC does it in software with certified firmware. Both the logic subsystem and the complete safety-related control system must be capable of achieving the required PLr. The PLr does not prescribe one specific Category; the achieved PL must be verified using the complete architecture and its safety data.

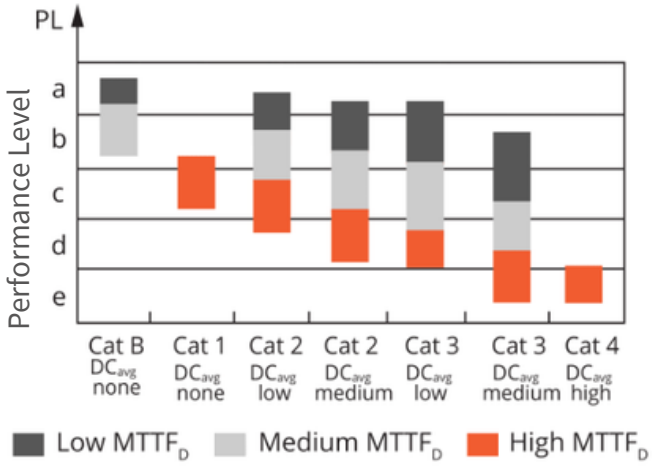
Now it's time to select the right components

Now that we have identified our hazards, it's time to select the correct safety components. A PLe-rated valve does not automatically create a PLe safety function.



The performance level of the overall safety function depends on the architecture, diagnostic coverage, fault detection, common cause failure considerations, and how all devices interact within the system.

Consider a light curtain installed too close to a hazard. The device may function exactly as designed, but if stopping distance was never evaluated, a person could still reach the hazard before motion stops.



The same failure mode exists with interlocked guards, pressure monitoring systems, and hydraulic safety circuits. A safety device is only effective when it is properly integrated into the overall safety function. The goal is not to install more safety products. **The goal is to reduce risk.**

Category, MTTFd, DC, and CCF: How They Work Together

These four parameters are not independent checkboxes. They interact to determine the achieved Performance Level (PLa), and understanding the tradeoffs between them is what separates good safety engineering from parts-swapping.

01 Category

Circuit architecture, single channel, redundant, with or without cross-monitoring

Implication

Sets the structural ceiling: a Category 2 architecture cannot achieve PLe

02 MTTFd

Mean Time to Dangerous Failure, component-level reliability

Implication

Higher MTTFd raises PL within a given Category; low MTTFd can drag down an otherwise sound architecture

03 DC (Diagnostic Coverage)

How thoroughly the system detects its own dangerous faults

Implication

Low DC limits PL even in high-Category systems; 90%+ DC required for **most** PL d applications

04 CCF (Common Cause Failure)

Vulnerability to a single event disabling both channels simultaneously

Implication

Must score ≥65 points using ISO 13849 checklist; separation, diversity, and filtering all contribute

Safety Components Available at Donald Engineering

All products are 3rd-party certified!

Safe Air Exhaust

DM2 Safety Valve

- *Cat. 4, PLe*
- *Internal Monitoring with Manual Reset*
- *B100: 20,000,000*

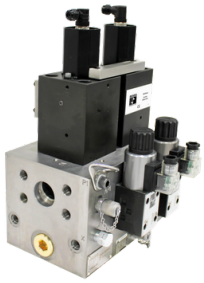
M35 Safety Valve

- *Cat. 4, PLe*
- *External Monitoring with & without Soft-Start*
- *B100: 25,000,000*

Hydraulic Valves

HBB Hydraulic Dual Block & Bleed Safety Valve

- *Cat. 4, PLe*
- *External Monitoring*



HBH RSE Hydraulic Block & Stop Safety Valve

- *Cat. 3, PLd*
- *Poppet-type cartridge valve elements*

Pneumatic Valves

CM26 Series Double Valves

- *Cat. 4, PLe*
- *Internal Monitoring, Manual reset*
- *Safe Return Valve*

EOAT

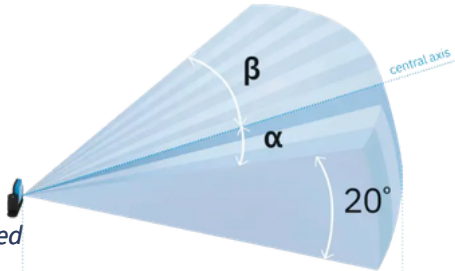
PGL-plus-P Universal Gripper with GripGuard

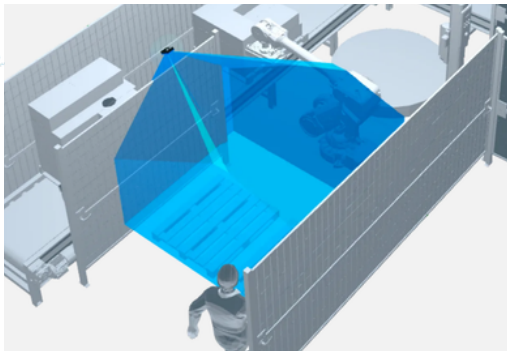
- *Cat. 3, PLd*
- *World's first & only safety-certified gripping force maintenance system.*

Radar Safety

S201A-W Safety Sensor

- *Cat. 3, PLd*
- *Safeguarding Presence Sensing*
- *Worlds first safety-certified radar system*





Many more component options & varieties are available. Please contact our team with questions.
The categories and performance levels shown are what these systems could be rated to, but it doesn't mean that if the entire system is used, it is at that level.

PART 2

Verify, Validate, & Document

Selecting components that should achieve the required PLr is not the same as having a system that does so. Verification and validation are two distinct activities that close that gap, and documentation is the record that proves the gap was closed.

VERIFICATION: Did We Design and Build It Right?

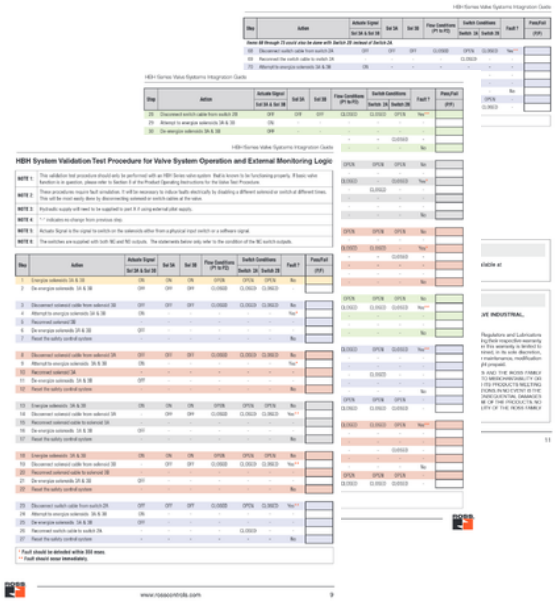
Verification is a design-level review, it happens on paper and in calculations before and during installation. It answers whether the system, as specified and built, matches the functional specification and PLr.
Key checks include:

- Do selected components carry certified functional safety data (MTTFd, DC, Category) from the manufacturer?
- Does the calculated PLa meet or exceed the PLr for every safety function?
- Is the circuit architecture (wiring, channel separation, monitoring connections) consistent with the required Category?
- Has Common Cause Failure (CCF) been scored and documented per ISO 13849-2?
- Does the functional specification account for all operating modes, including setup, maintenance, and fault recovery, not just normal production?

If any check fails, the design must be corrected before physical validation begins. Verification is a gate, not a formality.

VALIDATION: Does It Actually Work as Installed?

Validation is physical. It is performed on the machine, after installation, under real operating conditions. This is where calculations meet reality, and where assumptions get tested. Validation should be performed and signed off by a qualified safety professional, not by the person who did the installation.



See the example validation sheet from ROSS Controls in the Appendix.

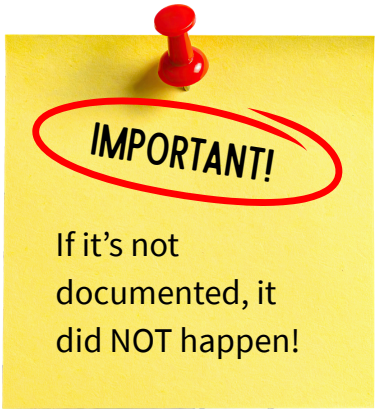
It should include:

- Trigger each safety function and confirm it activates correctly (E-stop, guard door, light curtain, pressure loss, etc.)
- Confirm each function holds the machine in a safe state and prevents restart until the proper manual reset sequence is completed.
- Inject faults deliberately: for example, disconnect one channel of a dual-channel system and confirm the second channel still performs the safety function and that the fault is detected and annunciated.
- Exhaustive – test all possibilities including wiring shorts and opens
- Test inputs as well as output devices
- Cycle the safety function repeatedly to confirm consistent performance, particularly for pneumatic systems where first-cycle behavior after a period of rest can differ from steady-state
- Measure actual response times (from trigger to safe state) and confirm they are within the stopping distances used in safe distance calculations

> ***If it isn't tested, it isn't proven.***
> *A dual-channel valve with one faulted spool will still exhaust, but through a different flow path, which increases exhaust time. If that extended response time was not accounted for in the safe distance calculation, an operator reaching into a hazard zone may not be protected even though the safety function technically "worked." Validation catches this. Calculations alone cannot.*

Documentation: The Record That Makes Everything Traceable

Documentation is one of the most overlooked parts of machine safety, and one of the most critical. It should not be treated as a paperwork exercise or assembled after the fact. Good documentation proves how safety decisions were made, what assumptions were used, how the system was verified, and how it was validated.



It also preserves intent: years after a machine is commissioned, operators and engineers change. **Without proper documentation, the reasoning behind critical safety decisions disappears with them.**

Document	Purpose
Risk Assessment	All task/hazard pairs with severity, frequency, and avoidance ratings are the foundation on which everything else is built.
Function Specification	Required safety functions, triggering conditions, required machine behavior, and boundaries of safe operation.
PLr Determination	ISO 13849 risk graph inputs and resulting PLr for each safety function.
Component Data Sheets	If available Certified MTTFd, DC, and Category data for every component in every safety function.
Achieved PLr Verification	SISTEMA output or equivalent showing PLa ≥ PLr for every safety function.
Circuit Diagrams	As-built architecture, including channel separation, monitoring connections, and feedback loops.
Validation Test Records	Signed and dated test results for every safety function, including fault injection results and measured response times

PART 3

Maintain It

A safety system that performs correctly on the day of validation is not automatically one that performs correctly two years (or two months) later. Valves wear. Sensors drift. Wiring gets disturbed during unrelated maintenance. People make changes without realizing they have affected the safety system. Maintenance is not optional, and it is not the same as general machine maintenance.

Periodic Testing: What It Means in Practice

Each safety function must have a defined inspection and functional-test interval. The interval should be based on the risk assessment, safety requirements specification, manufacturer instructions, applicable machine-specific standards, operating conditions, and assumptions used in the functional-safety calculation. Annual testing may be adopted as a facility standard, but some functions require more frequent testing and others may permit a longer interval.

> ***Example: Annual Guard Door Test***
> *Open the guard door while the machine is running. Confirm hazardous motion stops within the expected time. Confirm stored energy is removed or constrained. Confirm the machine cannot restart without the door closed and a deliberate manual reset. Measure and record the response time. Compare to the baseline from the original validation. Sign and date the record.* ***That is a maintenance test.***

If a safety system is partially disassembled during a line shutdown or upgrade, even if the change seems unrelated, the affected safety functions should be revalidated before the machine is returned to production. Most facilities that do this well build the revalidation step directly into their change management and PM procedures so it is never treated as optional.

When Does a Change Require a New Risk Assessment?

Not every change requires starting over, but some do. Under the ISO 12100 framework, the question is not *how much changed* but *what the change did to risk*. A modification requires a new risk assessment when it creates a new hazardous situation or increases an existing risk. The size of the rebuild, the number of components affected, or the intent behind the change are all secondary. **The only question that matters is: *did this change alter the safety picture*?**

Change Scenario	Key Question to Ask	Risk Assessment Needed?
Component replaced with comparable part	Does it behave identically in the same environment?	No — if function and performance are unchanged
Component replaced with alternative	Does the new component affect safety functions?	Yes — re-verify and re-validate
Machine relocated, layout changed	Are operator access paths, zones, or interfaces affected?	Yes — spatial changes alter risk profile
New tooling, product, or process introduced	Does operator interaction with the machine change?	Yes — safety functions were validated for original use
Software, drive parameters, or logic	Does the change affect machine behaviour or response?	Yes — code weighs as much as steel; validate logic
Guarding, access point, or operator interface added or changed	What was the underlying change that triggered this?	Evaluate the root cause — if access changes, reassess

A press that was validated for stamping one part is not automatically safe when it is retooled for a different part that changes the operator's interaction with the machine. The safety functions did not change, but the operator's interaction with the machine did, which means the hazard exposure changed. That is enough. The original validation documents tell you exactly what assumptions were made. **Which is why that documentation was worth building in the first place.**

BRINGING IT ALL TOGETHER

Machine Safety Isn't a Checklist. It's a System.

Throughout this series, we have built the complete machine safety process from the ground up. Every step in this process depends on the one before it. When the sequence is followed correctly, safety decisions become objective and traceable. When steps are skipped, the gaps do not disappear; they just become invisible until something goes wrong.

Step	What It Accomplishes
Risk Assessment	Identifies hazards, who is exposed, and how seriously
Design Out the Risk	Eliminates hazards at the source before protection measures are needed
Functional Specification	Defines exactly how the machine must respond when a hazard is detected
Performance Level Requirement (PLr)	Establishes how reliably those responses must occur
Select Mitigation Components	Chooses the hardware that achieves the required PLr as a complete, verified system
Validate, Verify & Document	Proves the system performs as designed and creates the traceable record
Maintain It	Ensures the system continues to provide the required level of protection over the life of the machine

Skip one step, and the entire system becomes weaker. The safest machines are not necessarily the ones with the most safety devices. They are the ones where hazards were understood, risks were evaluated, safety functions were clearly defined, protection measures were intentionally selected, and performance was verified, validated, documented, and maintained over time.

That's the difference between installing safety products and building a machine safety system.

HOW WE HELP

The Donald Engineering Difference

At Donald Engineering, we follow the ISO methodology because its structured and repeatable, giving machines the rigorous analysis that moves us towards safer machines and operations.

Schedule a Machine Safety Review, and we'll identify your top 2–3 risks and show you what a structured assessment looks like in your facility.

Contact our team today!

(616) 538-8340

sales@donaldengineering.com

APPENDIX 1: Ross Sample Validation Test Procedure

HBH System Validation Test Procedure for Valve System Operation and External Monitoring Logic

NOTE 1:	This validation test procedure should only be performed with an HBH Series valve system that is known to be functioning properly. If basic valve function is in question, please refer to Section 8 of the Product Operating Instructions for the Valve Test Procedure.
NOTE 2:	These procedures require fault simulation. It will be necessary to induce faults electrically by disabling a different solenoid or switch at different times. This will be most easily done by disconnecting solenoid or switch cables at the valve.
NOTE 3:	Hydraulic supply will need to be supplied to port X if using external pilot supply.
NOTE 4:	"-" indicates no change from previous step.
NOTE 5:	Actuate Signal is the signal to switch on the solenoids either from a physical input switch or a software signal.
NOTE 6:	The switches are supplied with both NC and NO outputs. The statements below only refer to the condition of the NC switch outputs.

Step	Action	Actuate Signal	Sol 3A	Sol 3B	Flow Conditions (P1 to P2)	Switch Conditions		Fault ?	Pass/Fail
		Sol 3A & Sol 3B				Switch 2A	Switch 2B		(P/F)
1	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	No	
2	De-energize solenoids 3A & 3B	OFF	OFF	OFF	CLOSED	CLOSED	CLOSED	-	
3	Disconnect solenoid cable from solenoid 3B	OFF	OFF	OFF	CLOSED	CLOSED	CLOSED	No	
4	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	Yes*	
5	Reconnect solenoid 3B	-	-	-	-	-	-	-	
6	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
7	Reset the safety control system	-	-	-	-	-	-	No	
8	Disconnect solenoid cable from solenoid 3A	OFF	OFF	OFF	CLOSED	CLOSED	CLOSED	No	
9	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	Yes*	
10	Reconnect solenoid 3A	-	-	-	-	-	-	-	
11	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
12	Reset the safety control system	-	-	-	-	-	-	No	
13	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	No	
14	Disconnect solenoid cable from solenoid 3A	-	OFF	OFF	CLOSED	CLOSED	CLOSED	Yes**	
15	Reconnect solenoid cable to solenoid 3A	-	-	-	-	-	-	-	
16	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
17	Reset the safety control system	-	-	-	-	-	-	No	
18	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	No	
19	Disconnect solenoid cable from solenoid 3B	-	OFF	OFF	CLOSED	CLOSED	CLOSED	Yes**	
20	Reconnect solenoid cable to solenoid 3B	-	-	-	-	-	-	-	
21	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
22	Reset the safety control system	-	-	-	-	-	-	No	
23	Disconnect switch cable from switch 2A	OFF	OFF	OFF	CLOSED	OPEN	CLOSED	Yes**	
24	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	-	
25	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
26	Reconnect switch cable to switch 2A	-	-	-	-	CLOSED	-	-	
27	Reset the safety control system	-	-	-	-	-	-	No	

* **Fault should be detected within 350 msec.**
** **Fault should occur immediately.**

HBH System Validation Test Procedure for Valve System Operation and External Monitoring Logic

APPENDIX

HBH Series Valve Systems Integration Guide

Step	Action	Actuate Signal	Sol 3A	Sol 3B	Flow Conditions (P1 to P2)	Switch Conditions		Fault ?	Pass/Fail
		Sol 3A & Sol 3B				Switch 2A	Switch 2B		(P/F)
28	Disconnect switch cable from switch 2B	OFF	OFF	OFF	CLOSED	CLOSED	OPEN	Yes**	
29	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	-	
30	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
31	Reconnect switch cable to switch 2B	-	-	-	-	-	CLOSED	-	
32	Reset the safety control system	-	-	-	-	-	-	No	
33	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	No	
34	Disconnect switch cable from switch 2A	-	-	-	-	-	-	-	
35	De-energize solenoids 3A & 3B	OFF	OFF	OFF	CLOSED	-	CLOSED	Yes*	
36	Reconnect switch cable to switch 2A	-	-	-	-	CLOSED	-	-	
37	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	-	
38	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
39	Reset the safety control system	-	-	-	-	-	-	No	
40	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	No	
41	Disconnect switch cable from switch 2B	-	-	-	-	-	-	-	
42	De-energize solenoids 3A & 3B	OFF	OFF	OFF	CLOSED	CLOSED	-	Yes*	
43	Reconnect switch cable to switch 2B	-	-	-	-	-	CLOSED	-	
44	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	-	
45	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
46	Reset the safety control system	-	-	-	-	-	-	No	
47	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	No	
48	Turn off and bleed supply to port P1	-	OFF	OFF	CLOSED	CLOSED	CLOSED	Yes**	
49	Turn supply back on to port P1	-	-	-	-	-	-	-	
50	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
51	Reset the safety control system	-	-	-	-	-	-	No	
52	Disconnect switch cable from switch 2A	OFF	OFF	OFF	CLOSED	OPEN	CLOSED	Yes**	
53	Attempt to reset the safety control system	-	-	-	-	-	-	-	
54	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	-	
55	Reconnect the switch cable to switch 2A	-	-	-	-	CLOSED	-	-	
56	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
57	Reset the safety control system	-	-	-	-	-	-	No	
58	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	-	
59	De-energize solenoids 3A & 3B	OFF	OFF	OFF	CLOSED	CLOSED	CLOSED	-	
60	Disconnect switch cable from switch 2B	OFF	OFF	OFF	CLOSED	CLOSED	OPEN	Yes**	
61	Attempt to reset the safety control system	-	-	-	-	-	-	-	
62	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	-	
63	Reconnect the switch cable to switch 2B	-	-	-	-	-	CLOSED	-	
64	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
65	Reset the safety control system	-	-	-	-	-	-	No	
66	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	-	
67	De-energize solenoids 3A & 3B	OFF	OFF	OFF	CLOSED	CLOSED	CLOSED	-	

*** Fault should be detected within 350 msec.**
**** Fault should occur immediately.**

HBH System Validation Test Procedure for Valve System Operation and External Monitoring Logic

APPENDIX

Step	Action	Actuate Signal Sol 3A & Sol 3B	Sol 3A	Sol 3B	Flow Conditions (P1 to P2)	Switch Conditions Switch 2A	Switch 2B	Fault ?	Pass/Fail (P/F)
Items 68 through 75 could also be done with Switch 2B instead of Switch 2A.									
68	Disconnect switch cable from switch 2A	OFF	OFF	OFF	CLOSED	OPEN	CLOSED	Yes**	
69	Reconnect the switch cable to switch 2A	-	-	-	-	CLOSED	-	-	
70	Attempt to energize solenoids 3A & 3B	ON	-	-	-	-	-	-	
71	Attempt to reset the safety control system	-	-	-	-	-	-	-	
72	De-energize solenoids 3A & 3B	OFF	-	-	-	-	-	-	
73	Reset the safety control system	-	-	-	-	-	-	No	
74	Energize solenoids 3A & 3B	ON	ON	ON	OPEN	OPEN	OPEN	-	
75	De-energize solenoids 3A & 3B	OFF	OFF	OFF	CLOSED	CLOSED	CLOSED	-	

** Fault should occur immediately.

CAUTIONS, WARNINGS

Additional technical documentation, cautions and warnings information is available at www.rosscontrols.com, Support and Downloads.

STANDARD WARRANTY

ROSS OPERATING VALVE, ROSS CONTROLS®, ROSS DECCO®, and AUTOMATIC VALVE INDUSTRIAL, collectively the "ROSS Family".

All products sold by the ROSS Family are warranted for a one-year period [with the exception of Filters, Regulators and Lubricators ("FRLs") which are warranted for a period of seven (7) years] from the date of purchase. All products are, during their respective warranty periods, warranted to be free of defects in material and workmanship. The ROSS Family's obligation under this warranty is limited to repair, replacement or refund of the purchase price paid for products which the ROSS Family has determined, in its sole discretion, are defective. All warranties become void if a product has been subject to misuse, misapplication, improper maintenance, modification or tampering. Products for which warranty protection is sought must be returned to the ROSS Family freight prepaid.

THE WARRANTY EXPRESSED ABOVE IS IN LIEU OF AND EXCLUSIVE OF ALL OTHER WARRANTIES AND THE ROSS FAMILY EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES EITHER EXPRESSED OR IMPLIED WITH RESPECT TO MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE ROSS FAMILY MAKES NO WARRANTY WITH RESPECT TO ITS PRODUCTS MEETING THE PROVISIONS OF ANY GOVERNMENTAL OCCUPATIONAL SAFETY AND/OR HEALTH LAWS OR REGULATIONS. IN NO EVENT IS THE ROSS FAMILY LIABLE TO PURCHASER, USER, THEIR EMPLOYEES OR OTHERS FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES WHICH MAY RESULT FROM A BREACH OF THE WARRANTY DESCRIBED ABOVE OR THE USE OR MISUSE OF THE PRODUCTS. NO STATEMENT OF ANY REPRESENTATIVE OR EMPLOYEE OF THE ROSS FAMILY MAY EXTEND THE LIABILITY OF THE ROSS FAMILY AS SET FORTH HEREIN.

HBH System Validation Test Procedure for Valve System Operation and External Monitoring Logic