FGD Common Absorber and Boiler Operations Safety

Henry A. Sierk, Jr.

and

Phillip Wang

Boiler safety can be a concern when connecting multiple units to a common absorber. This paper addresses a safety instrumented system approach to boiler / furnace safety including implosion protection.

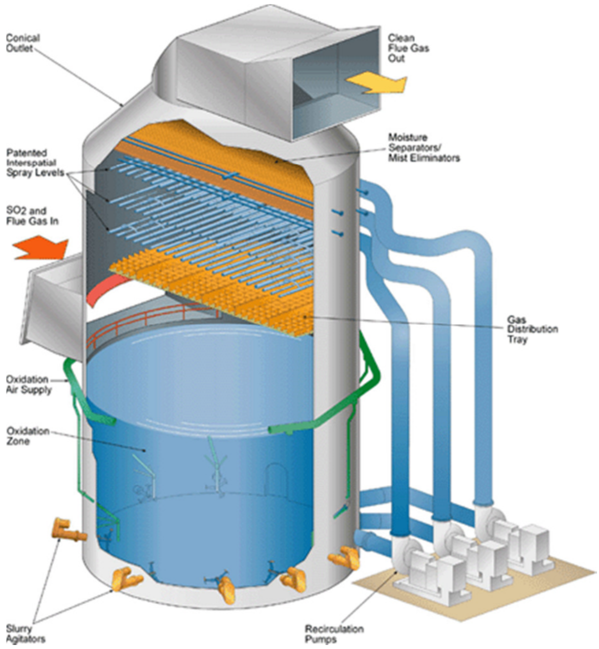
Dominion Resources
5000 Dominion Boulevard
Glen Allen, VA

Microfusion Engineering Laboratories, Inc
3250-E Peachtree Corners Circle
Norcross, GA 30092

12/11/2012

Overview – Original Concept

As a part of its environmental improvement strategy, Dominion added wet flue gas desulphurization (FGD) equipment to four coal-fired boilers at the Chesterfield Power Station in Virginia. This project was in the planning stages in 2004, construction began in 2006 and was completed in 2012. The project consists of two roughly identical Siemens wet slurry absorbers each with a capability to scrub approximately 700 MW of generation utilizing high sulfur coal. The first system was installed for the largest unit at the plant, Unit 6, with a net capability of about 652 MW. This portion of the project was completed in 2008. The second system followed commissioning of the Unit 6 system and was designed to scrub the remaining three coal units at the plant with net capabilities of approximately 325 MW, Unit 5, 166 MW, Unit 4 and 100 MW, Unit 3. The total of these three units is 591 MW, a similar combined rating to Unit 6.



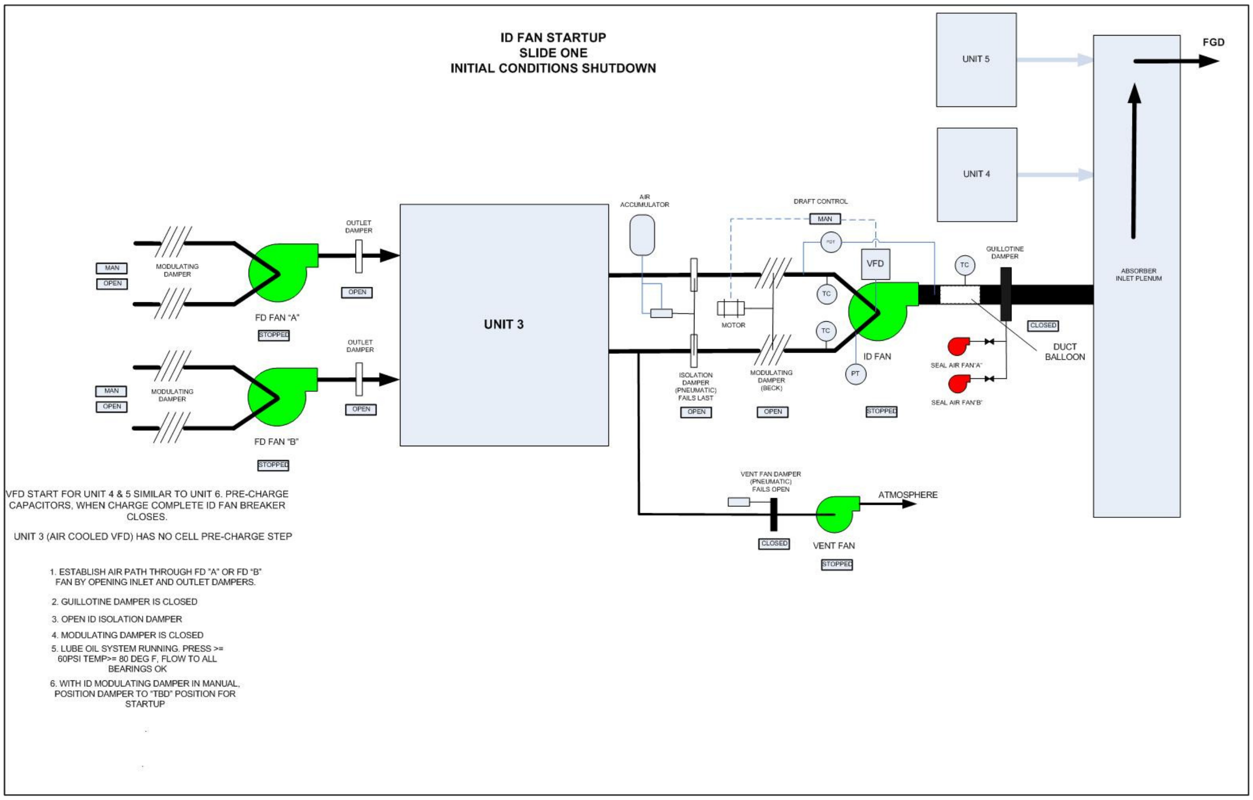
The Chesterfield station is located along the James River about 15 miles south of Richmond. Including two gas/oil fired combined cycle units, the station can generate more than 1600 megawatts and is the largest fossil-fueled power station in Virginia.

The plant is located along the river which serves as its source of cooling water. The area between the boilers and the river had become congested over the years from additions of larger precipitators, Selective Catalytic Reducers for NOx removal, limestone injection systems, larger ID fans to support this equipment and other plant systems. As a result the area needed for installation of the FGD equipment was extremely limited. Considering the projected capacity factors of these units at the time, the decision was made to install new variable speed ID fans before the planned tie-in outages. These new fans would then be connected to the boiler and the new absorber during the outages. The old fans and associated equipment could then be removed after the tie-in outages. This approach was designed to shorten the required outage windows by 4 to 6 weeks per unit.

Considerations regarding the outage plans, the capacity factors of the older units and the limited space led to decisions to go with one ID Fan for each of the older units (Unit 3, built in 1952 and Unit 4, built in 1960). Unit 5, a relative youngster starting its career in 1964, was elected to retain two fans in accordance with its original design. The decision was made to utilize variable speed fans as had been the design concept for Unit 6 to offset some of the additional power requirements resulting from the FGD equipment. Units 4 & 5 were supplied with Siemens water cooled, 5000 HP Variable Frequency Drives (VFD). Unit 3 was supplied with a Siemens 2500 HP air cooled VFD.

The discharge from each unit’s ID Fan flows into a common absorber inlet duct which operates at a positive pressure of 6 to 8 inches water column. Maintenance isolation was provided via a motorized guillotine damper at the ID Fan outlet. This serves to isolate the unit from the common duct. To provide boiler ventilation for maintenance purposes a fan was designed to take suction from the ID Fan inlet upstream of the modulating inlet damper and discharge to atmosphere. This maintenance fan was designed to have local control only. Because the guillotine dampers served no control purpose, their speed was very slow, opening (or closing) in about 5 minutes. The modulating ID Fan inlet dampers were designed for furnace pressure control at low flows when the ID Fan is operating at minimum speed (about 30% of full speed). The operating speed of these dampers allows them to full stroke in 15 seconds.

A simplified sketch of Unit 4 is shown here, as originally designed:


ID FAN STARTUP
SLIDE ONE
INITIAL CONDITIONS SHUTDOWN

VFD START FOR UNIT 4 & 5 SIMILAR TO UNIT 6. PRE-CHARGE CAPACITORS, WHEN CHARGE COMPLETE ID FAN BREAKER CLOSES.

UNIT 3 (AIR COOLED VFD) HAS NO CELL PRE-CHARGE STEP

1. ESTABLISH AIR PATH THROUGH FD "A" OR FD "B" FAN BY OPENING INLET AND OUTLET DAMPERS.
2. GUILLOTINE DAMPER IS CLOSED
3. OPEN ID ISOLATION DAMPER
4. MODULATING DAMPER IS CLOSED
5. LUBE OIL SYSTEM RUNNING. PRESS >= 60PSI TEMP>= 80 DEG F, FLOW TO ALL BEARINGS OK
6. WITH ID MODULATING DAMPER IN MANUAL, POSITION DAMPER TO "TBD" POSITION FOR STARTUP

Please note that the pneumatic inlet dampers shown here were not in the original design.

Plans were in place to stiffen all boiler structures to +/- 35 inwc in accordance with NFPA 85 recommendations. This was expected to be a very expensive effort, particularly on the older two units. The peak ID Fan head capabilities of the new fans were in the range of 40 to 48 inches water column. This was far beyond the pressure capabilities of the boiler casings based on the available information. Dominion had records that Unit 5 boiler, ductwork and precipitator had been modified during a previous environmental project to meet the +/- 35 inwc design maximums recommended by NFPA. Unit 4 had been modified during a previous precipitator upgrade project to +/- 20 inwc. Unit 3 was believed to be rated at +/- 13 inwc because those were the settings of the furnace pressure fan trips, however, no historical documentation could be found to verify this. While NFPA limits the design pressure at +/- 35 or the fan head, whichever is lower, Dominion believed that there was still room for concern based on the capabilities of the new fans. Our investigation also indicated that Alstom (the boiler manufacturer) used +/- 35 not as a design point (with some assumed margin) but as a yield point when they upgraded Unit 5 structure.

Process Safety Concerns

Early in the design process for the Units 3-4-5 FGD system, Dominion Engineering expressed concern over the safety of the process. These expressed concerns led to meetings with Dominion’s Environmental Projects group; an outside review with an independent A/E firm and finally a joint meeting of the projects group with internal experts from operations and engineering.

The concerns centered around two areas. First, there was a concern over the inability to perform a natural boiler post-purge on loss of all fans. In the original plant design, ID Fans discharged directly into a roughly 200 foot chimney. If all fans tripped for any reason, a coast down timer would hold dampers in their last position allowing the fans to slow sufficiently to prevent damage to the boiler, then all fan dampers would drive wide open and be held open for 15 minutes to provide for a natural boiler purge. In this scenario, the heat in the boiler and chimney would cause flow up to the stack outlet because the air was lighter than the surrounding air. Pulverizer flow control dampers would close to a minimum position that would allow a slight draft due to furnace air flow to remove any methane produced by the hot fuel trapped inside. This simple methodology had been effective for many years of plant operation.

The environmental upgrade project introduced two process-related problems. First was the fact that there would be only one ID Fan on each of the older units. This doubles the likelihood of an all fans off condition, since loss of this one fan would need to trip both FD Fans. Added to this, the ID Fan would now utilize a VFD which could only increase the probability of an ID Fan trip by the mere fact that there is another piece of equipment involved. Secondly, the boiler cannot vent naturally into a chimney but rather must be pumped into a common header that runs at a significantly positive pressure.

The second area of concern is that of negative furnace pressure transients great enough to structurally deform the boiler casing. This is the implosion concern mentioned above. Additionally, the Dominion Environmental Projects group was interested in determining the practicability of providing controls to prevent implosion rather than physical boiler modifications to reduce overall project capital cost.

In May of 2009, a modeling study was initiated to determine the effects of various operating transients and their impact on furnace pressure. The company performing the modeling was Microfusion Engineering Laboratories. The decision was made to model Unit 4 since it had the ID Fan with the highest total head capability (48 inwc). Microfusion developed two independent models, one using their own THINK-4^{TM} process simulation code and a second using STAR-CCM+ Computational Fluid Dynamics code. Each model was designed using the actual volumes and flow paths through the furnace, SCR, Precipitator and ductwork and using the actual fan curves for the ID and FD fans. The actual ID Fan inertia was utilized to determine the fan roll down time under load and the peak pressures possible if the fan were tripped. The models were manipulated to determine the ideal speed of the control devices to minimize possible transients. From the modeling, it became immediately apparent that a high speed process element at the ID Fan was beneficial to reduce transients. Also, slower final control elements at the supply side reduce the possibility of delivery based implosion event. One new concern that had to be addressed was the possibility of an ID Fan speed run-away. This was conceived to be some kind of failure either in the demand signal going to the VFD or within the control mechanism of the VFD proper that would cause the fan speed to go to maximum.

Microfusion issued their initial report in August of 2009. Subsequent modeling cases requested by Dominion extended the final modeling work into November. At this point, the basis for the Safety Instrumented System and associated process equipment changes had been confirmed.

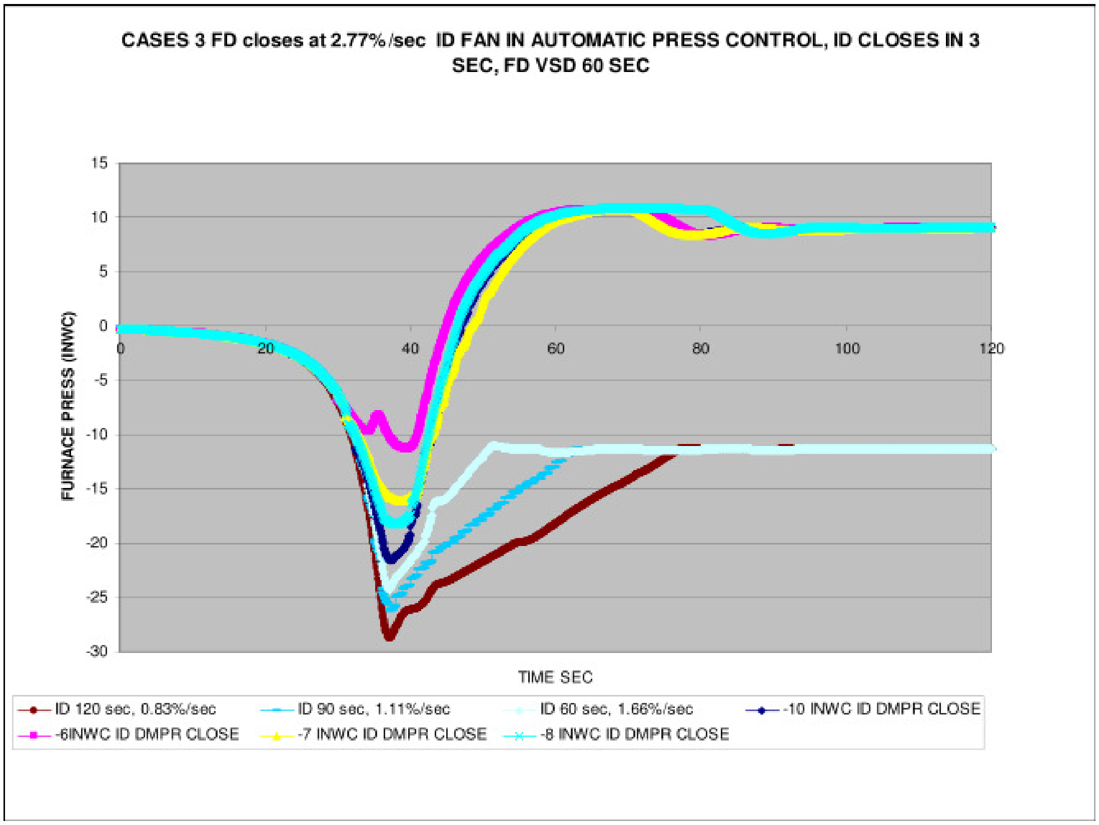
The outcome of this study was to determine that it was possible to control the peak negative pressure achievable by addition of a set of fast closing ID Fan inlet dampers and by limiting the speed of the FD Fan dampers and windbox dampers. It appeared that a design target of 4-5 seconds for closing the ID Fan Inlet Dampers was desirable.

The following is the output from one of the many model runs. In this model run, the FD fans were closed at maximum rate of 2.77%/sec and the ID Fan furnace pressure control was in automatic. Cases included stopping the ID Fan rotor in 60, 90 and 120 seconds or closing a fast inlet damper at -6, -7, -8 or -10 inwc. This shows that either closing the inlet damper sooner or stopping the fan at a higher rate both benefit the process with smaller peak negative pressures.

Rev. 1.0	ENGINEERING CALCULATIONS AND ANALYSIS REPORT						
Report No.:	Dom-37-02	Report Rev. No.:	Rev. 1.0	Project File No.:	Chesterfield	Date:	Nov 2009
Title: [m]	Analysis of Chesterfield Unit 4 ID Fan Dynamics Final Report						

Case 6 Graph

Cases 6 involved closing the FD fan damper while letting the ID fan roll down (in 60, 90, 120 sec) to 0 rpm. Also closing the ID isolation damper (in 3 sec) when the furnace pressure drops below –6, -7, -8, -10INWC.



Process Hazards Analysis

Since a controls-based solution would definitely need to be a Safety Instrumented System (SIS) and our experience with this type of system in power generation was very limited, Dominion decided to bring a professional Process Hazards Analysis (PHA) firm into the project. A consultant was hired and Dominion assembled an internal team to perform the process risk assessment with the consultant acting as the facilitator. The team consisted of representatives from corporate loss prevention, engineering, plant operations and plant instrumentation maintenance. This team met over a one week period to develop the system and evaluate the probability of failure on demand (PFD) for each component. PFDs were calculated based on plant experience or utilizing the consultant's database where Dominion data was lacking.

The major concern going into this analysis was furnace implosion and furnace explosion was also to be considered. The PHA numerical analysis identified furnace explosion as the higher concern and implosion as secondary. This was due primarily to the extent of the effects of these events. Implosion was considered to have effects in a limited area, the area of structural failure, which would then relieve the forces causing the damage. Boiler explosion, on the other hand, would have far reaching effects. So although the probability of explosion was lower, the potential for human impact and secondary effects such as damage to adjacent boilers and environmental issues was higher.

From previous studies and this analysis, the following process changes were implemented:

- **Fast Acting Inlet Dampers** were added to all ID Fans. These were pneumatically operated, open/close dampers with redundant solenoids, a local air receiver sized for 5 operations, and SIL rated hardware. These dampers were provided with positioners to allow for partial stroke testing when the unit is on line and with SIL rated proximity switches for end of travel determination. These are a completely separate set of dampers from the modulating dampers originally included.

- **ID Fan Dynamic Braking** was added to all VFDs. Modeling showed that slowing the ID Fan more rapidly reduced the potential negative furnace pressure transient. This was considered to be a backup to the Fast Acting Inlet Dampers. Since it utilized a completely separate control mechanism, the possibility of common mode failure would be reduced. Plant personnel preferred an electronic protection system since mechanical equipment (dampers) in a challenging environment have evidenced a high potential for failure.

  One of the difficulties here is that Units 4 & 5 utilized a VFD design that had capability for full regenerative braking. The target for this braking was to reduce fan speed to less than half of the speed prior to the event in 5 seconds. This is based on the fact that head produced by the fan is a function of the square of the speed. This would require braking from full speed to stop in about 10 seconds.

Unit 3 VFD was a different design and did not have this capability. Our information from the supplier seemed to indicate that braking was possible utilizing a dual-frequency methodology. Later it was determined that this drive could not regenerate any power back to the power source, but could only absorb power temporarily in the drive. This severely limited the braking capability for this fan.

- **Removal of FD Fan Outlet Dampers** – FD Fan outlet dampers can close due to a logical error or equipment failure and cause an implosion event. Practice has shown that these dampers are unnecessary.

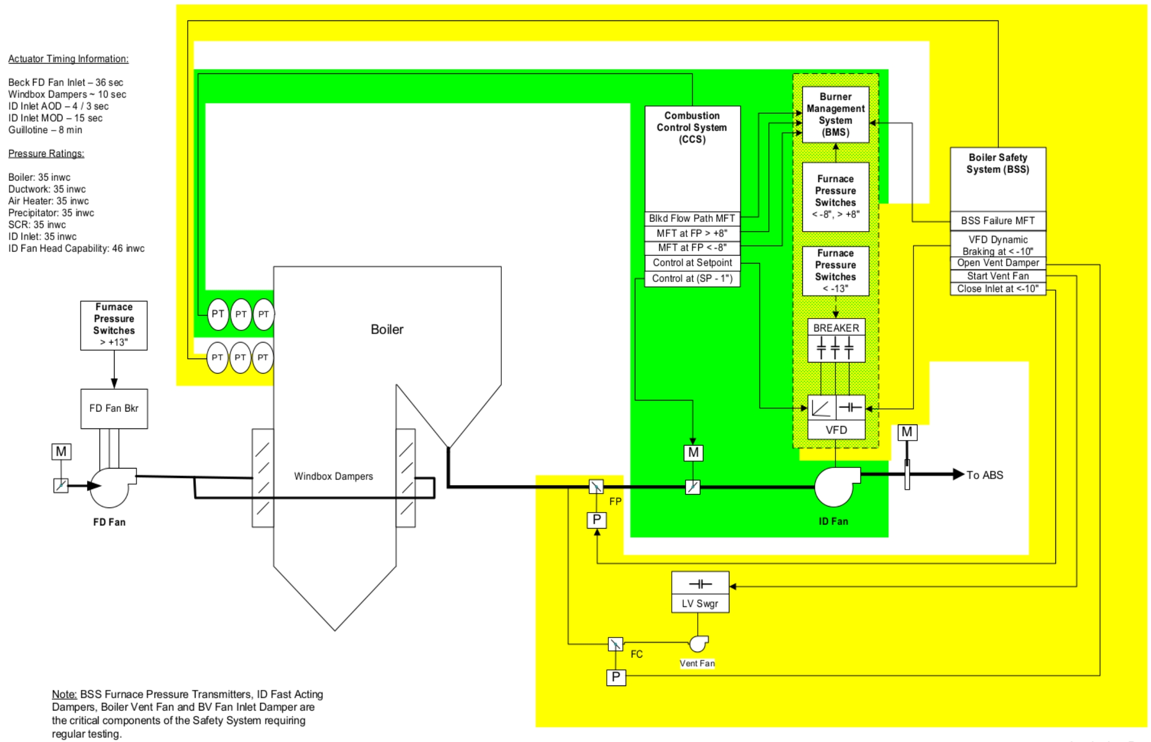
- **Automation of the Purge Fan** – The maintenance fan originally provided for outage work was automated to perform post-purge operations. As a result it was renamed the Purge Fan. This automation involved a number of changes. The fan motor starter was modified for automatic starting in a fail-safe mode. This means that on a control failure, the fan will start. The fan had to be modified to allow for handling hot gases and for running in test mode with the unit on line. Additionally, the fan was equipped with an anti-rotation clutch to prevent "free wheeling" when tested. The inlet damper was automated with redundant close solenoids and the required equipment to allow for testing operation with the unit on line. Finally, a full complement of fan instrumentation was added to these fans due to their critical function. This included vibration sensing, fan differential pressure, bearing temperatures, and motor stator temperatures.

- **Additional Purge Fan** – On units 3 & 4, which were retrofitted with only one ID Fan, a second Purge Fan was added due to the higher probability of an all fans off event.

- **Fuel Shutoff** – On units 3 & 4, for the reasons stated above, acceptable risk targets could only be achieved by adding another independent layer of protection. It was determined that the best possible benefits could be achieved by fuel shutoff. Normally, on these units, a boiler trip stops all mills and exhausters, however the exhausters will spin down due to their rotating mass. The mills would continue to deliver fuel to the furnace during their coast down for 10 to 15 seconds. Adding fast closing slide gates to the exhauster outlets could stop fuel flow in a couple of seconds thereby reducing the inventory of unburned fuel in the furnace if boiler post-purging were to fail.

- **Mill Inerting** – Fuel shutoff introduces another hazard by preventing the venting of methane gases that would result from the presence of fuel, heat and oxygen in the mills following a trip. To reduce this risk, a CO_2 inerting system was installed on these mills. This would be designed to displace oxygen in the mills with CO_2 and prevent methane formation as well as eliminate the potential for mill fires.

The concept evaluated by the team is approximately as shown on the following diagram:



Note: BSS Furnace Pressure Transmitters, ID Fast Acting Dampers, Boiler Vent Fan and BV Fan Inlet Damper are the critical components of the Safety System requiring regular testing.

Implosion Protection
Diagram, Rev 2

SIL Determination

The first, and most difficult effort was to determine our corporate risk tolerance. This is a number often in the range of 10^{-6} and is the tolerance for a catastrophic event involving loss of life. Since this is a very difficult subject, companies are desirous to say that this number is zero. However, zero is certainly not achievable in a real world situation and complexity (and cost) increases asymptotically as the number becomes smaller. The following are some sample fatality probabilities taken from a table in the ISA book "Safety Instrumented Systems, 2nd Edition."

Air Travel	2×10^{-6}
Automobile Travel	2×10^{-4}
Cancer	1×10^{-6}
Fire	2.5×10^{-5}

The risk tolerance is actually a table of probabilities which might define different severities and their associated tolerance probability.

Once this is determined, the effort centers on assessing every possible initiating cause and potential frequency of that initiating cause. Then, one must assess the probability of failure on demand (PFD) of each independent layer of protection. This is a difficult process and requires active involvement of all team members. Sources of data can be plant experience, maintenance records, general industry data, etc. Ultimately, each initiating cause frequency is multiplied by the PFD of each independent layer of protection that affects that cause and an overall event frequency for that cause is determined. Each initiating cause is similarly assessed and the total of all the overall event frequencies is compared against the corporate tolerance for that event. If the total event frequency is higher than the corporate risk tolerance, an additional layer of protection needs to be added that will reduce the frequency to the corporate tolerance or lower. The PFD of this added protection layer determines the Safety Integrity Level (SIL) rating of the safety system.

By the IEC 61511 standard, SIL levels are determined as follows:

Safety Integrity Level	**Probability of Failure on Demand**
SIL 1	0.1 to 0.01
SIL 2	0.01 to 0.001
SIL 3	0.001 to 0.0001
SIL 4	0.0001 to 0.00001

In practice, SIL 3 or 4 systems are very rare. The complexity and cost of such systems are unreasonable and hence are avoided.

In our evaluation of explosion risk, a Layers of Protection Analysis (LOPA) was performed. The table looks something like this:

PFDavg Calculation

Initiating Cause	Freq (yrs)	Independent Layers of Protection								
		1	2	3	4	5	6	7	8	I.E.F(/yr)
A	.0008	0.10000	0.50000	1.00000	0.25000					1.0E-5
B	0.00027	0.10000	0.50000	1.00000	1.00000					1.4E-5
C	3.8E-6	0.10000	0.50000	1.00000	1.00000					1.9E-7
D	0.001	0.10000	0.50000	1.00000	1.00000					5.0E-5
E	0.0038	0.10000	0.50000	1.00000	1.00000					1.9E-4
F	0.00001	0.10000	0.50000	1.00000	1.00000					5.0E-7
G	0.0022	0.10000	0.50000	0.10000	1.00000					1.1E-5
H	0.008	0.10000	0.50000	0.10000	1.00000					4.0E-5
I	0.001	0.10000	0.50000	1.00000	1.00000					5.0E-5
J	0.03	0.01000	0.50000	1.00000	1.00000					1.5E-4
K	0.00007	0.10000	0.50000	0.10000	0.25000					8.8E-8

	Total Event Frequency Fe/yr.	5.2E-4
	PFDavg for Safety Instrumented Function, Ft/Fe	3.9E-3
	Safety Integrity Level =	SIL 2
Comments	1. Further information on the initiating causes and independent layers of protection is given in Section x.x of the Furnace Safety Integrity Level Assessment Report.	

The values in this table are representative only for purposes of understanding the process and are not representative of the final analysis.

The following are some of the initiating causes that were considered in the analysis:

- Loss of ID Fan – Failure of VFD
- Loss of ID Fan – Lube Oil Failure
- Motorized Inlet Damper Closed – Drive Failure
- Motorized Inlet Damper Closed – DCS Failure
- Motorized Inlet Damper Closed – Operator Error
- Pneumatic Inlet Damper Closed – Human Error During Maintenance
- Guillotine Damper Closed – Operator Error
- Guillotine Damper Closed – DCS Error
- Furnace Pressure Measurement Fails
- Total Unit Power Failure
- Failure to Determine Fan Running Status

Independent Layers of Protection considered were:

- Flammable atmosphere may not occur or ignite
- Avoidance / Occupancy
- Operator Response to Guillotine Damper Closing
- Operator Response to VFD Alarms

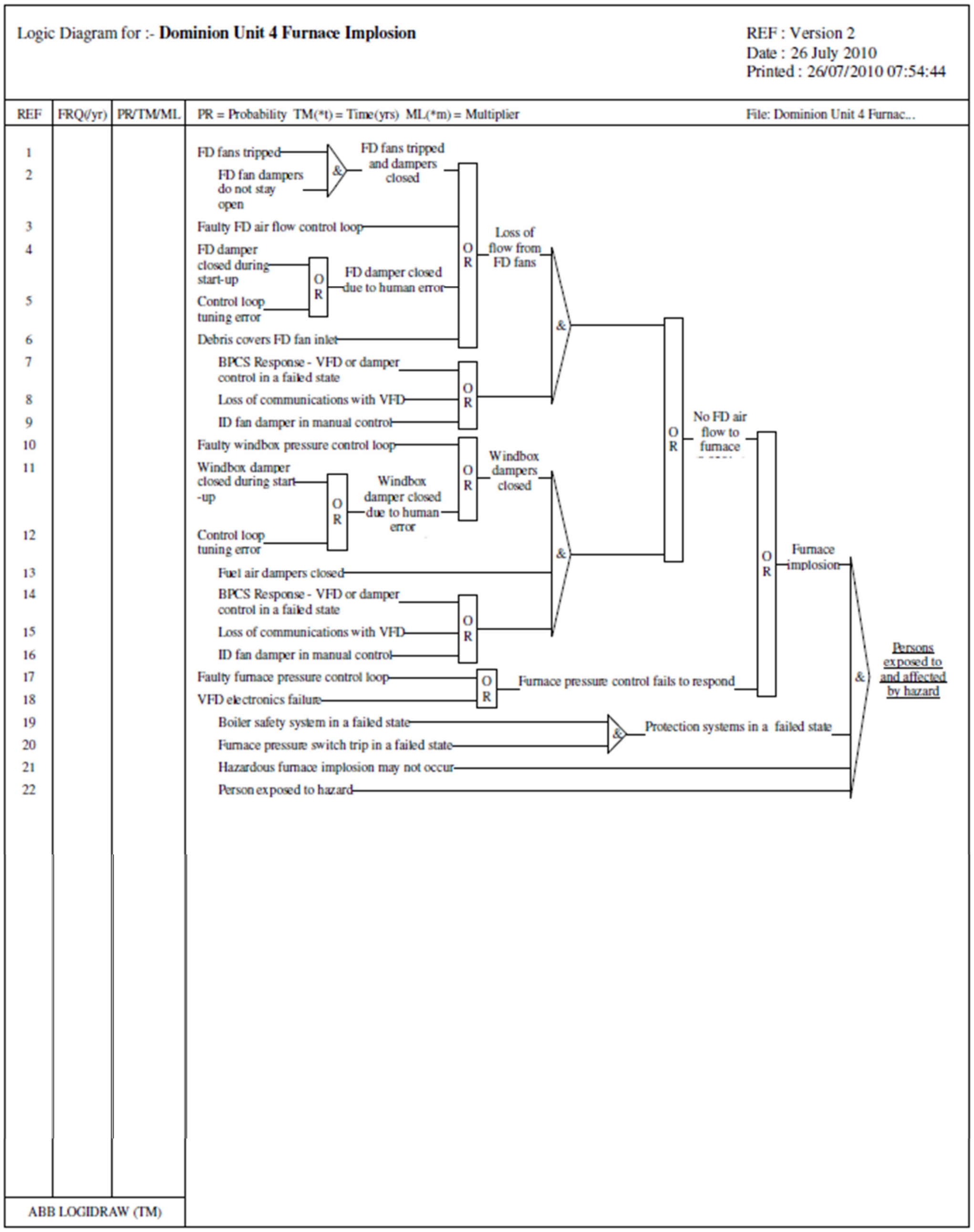
Documentation of each initiating cause and the justification for the frequency used is essential. The consultant provided software to keep this form of documentation and the following is one example of the associated documentation for a loss of ID Fan due to lube oil failure:

> Each fan is served by two lube oil pumps operating on a duty / standby with auto cut in of the standby unit. Catastrophic failure of the fan is unlikely to occur on loss of lube oil and the operators would have time to initiate a controlled shutdown.
>
> Assume for each ID fan that the lube oil pumps fail at a frequency of 0.2 per year. Conservatively assume a maximum of 15 days of undetected failure of the standby unit. Failure rate = f1.f2(t1 + t2) where f= fan failure frequency per year and t = undetected failure duration. F = 0.2 * 0.2 * (15/365 + 15/365) = 0.0033 per year. Assume probability of 0.1 of operator failure to respond to BPCS alarm (based on more than 10-15 minutes if action from control room). Frequency of failure of both lube pumps on one ID fan = 0.0003 per year. Assume probability of 0.1 of operator failure to respond to BPCS alarm (based on more than 10-15 min if action from control room). Overall frequency = 3E-05 per year. As each fan is served by two lube oil pumps, all 4 pumps need to fail for the event to occur. Conservatively apply an additional factor of 0.1 to account for this, giving an overall failure frequency of 3.3E-06 per year

Once again, the numbers are only representative.

Similarly, the independent layers of protection are documented with appropriate justifications.

On this project a more stringent fault tree analysis was performed for the implosion protection. This was chosen for implosion because this was the first assessment and at the beginning of the process was our higher concern. This allows a more structured assessment considering the logical relationship of protection layers on initiating causes. This analysis method can provide more accurate results but is more time consuming. An example fault tree is shown below. All values for frequencies and probabilities have been removed.


Logic Diagram for :- Dominion Unit 4 Furnace Implosion
REF : Version 2
Date : 26 July 2010
Printed : 26/07/2010 07:54:44
REF
FRQ(/yr)
PR/TM/ML
PR = Probability TM(*t) = Time(yrs) ML(*m) = Multiplier
File: Dominion Unit 4 Furnac...
1 FD fans tripped
2 FD fan dampers do not stay open
FD fans tripped and dampers closed
3 Faulty FD air flow control loop
4 FD damper closed during start-up
5 Control loop tuning error
FD damper closed due to human error
6 Debris covers FD fan inlet
Loss of flow from FD fans
7 BPCS Response - VFD or damper control in a failed state
8 Loss of communications with VFD
9 ID fan damper in manual control
10 Faulty windbox pressure control loop
11 Windbox damper closed during start -up
12 Control loop tuning error
Windbox damper closed due to human error
Windbox dampers closed
13 Fuel air dampers closed
14 BPCS Response - VFD or damper control in a failed state
15 Loss of communications with VFD
16 ID fan damper in manual control
No FD air flow to furnace
17 Faulty furnace pressure control loop
18 VFD electronics failure
Furnace pressure control fails to respond
Furnace implosion
19 Boiler safety system in a failed state
20 Furnace pressure switch trip in a failed state
Protection systems in a failed state
21 Hazardous furnace implosion may not occur
22 Person exposed to hazard
Persons exposed to and affected by hazard
OR
&
ABB LOGIDRAW (TM)

Safety Requirements Specification

From the PHA and SIL analysis, Dominion developed a Safety Requirements Specification based on the IEC 61511 requirements. Defining these requirements helped us to think through many of the areas that might not be considered in designing normal process controls. Some of these are the following:

- Considerations relating to common cause failures
- Detailed determination of process safe states for all outputs
- Proof testing
- Energized versus de-energized to trip
- Interfaces with the Basic Process Control System (BPCS, ie. DCS)
- Resetting the SIF after activation
- Overrides and inhibits allowed
- Dangerous combinations of outputs

It was very important to consider carefully what functions were performed in the BPCS and what was operated by the safety system.

The BPCS (DCS) performed normal furnace pressure control using the ID Fan speed or inlet damper as appropriate. It also controlled the guillotine damper, ID Fan lube oil systems and associated monitoring and alarming.

We determined that the following devices would be controlled by the safety system:

- ID Fan Dynamic Braking Command
- ID Fan VFD Breaker Control
- ID Fan Inlet Fast Acting Damper
- Boiler Purge Fan(s)

The safety system needs to be completely independent of the BPCS and must not share common failure modes. This led to some interesting design decisions. One example of this independence was separate pressure taps, wiring paths and power to the furnace pressure transmitters used for the safety system. Transmitters for the BPCS and the safety system were purchased from different manufacturers to eliminate any possible common mode transmitter software issues.

Along these lines the safety system although supplied by the same company, utilized hardware that was designed for SIL applications and was completely different from that used in the BPCS.

Equipment safe states generated some interesting issues. Our analysis determined that the safe state for the Boiler Purge Fan(s) was running. This meant that the design called for these motors to start on SIF actuation, loss of power to the interposing relays or a complete failure of the safety system. This required special precautions to be developed for maintenance personnel who might need to work on the breakers or the fans. Also, unavailability of the Boiler Purge fans makes the safety system functionally unavailable. As a result it was necessary to determine a maximum period of unavailability before a generating unit shutdown is mandated.

Proof testing also was a complicated affair. The standards make it clear that a safety system that is not tested cannot be considered to be available. Boiler purge fans, with some modifications, could be tested with the generating unit in service, but clearly it is not possible to close the ID Fan inlet damper or initiate ID Fan dynamic braking with the unit in service. Dominion decided to handle this by requiring system functional testing annually and also as a logical pre-requisite to boiler purge any time a unit is started. Partial stroke tests on the ID Fan inlet damper, Purge Fan tests and Furnace Pressure Transmitter tests are required monthly. Automated test sequences were developed to validate each portion of the safety system. For example, safety system furnace pressure transmitters are tested monthly by storing 15 seconds worth of data on each then offsetting the furnace pressure setpoint in the BPCS by -1 inwc. The safety system allows 20 seconds to reach the new pressure setpoint, then 15 seconds of data is again stored on each transmitter. If the average pressure on each of the three transmitters doesn’t change in the correct direction by at least 60% of the setpoint change, the test fails. The following tests were developed and validated:

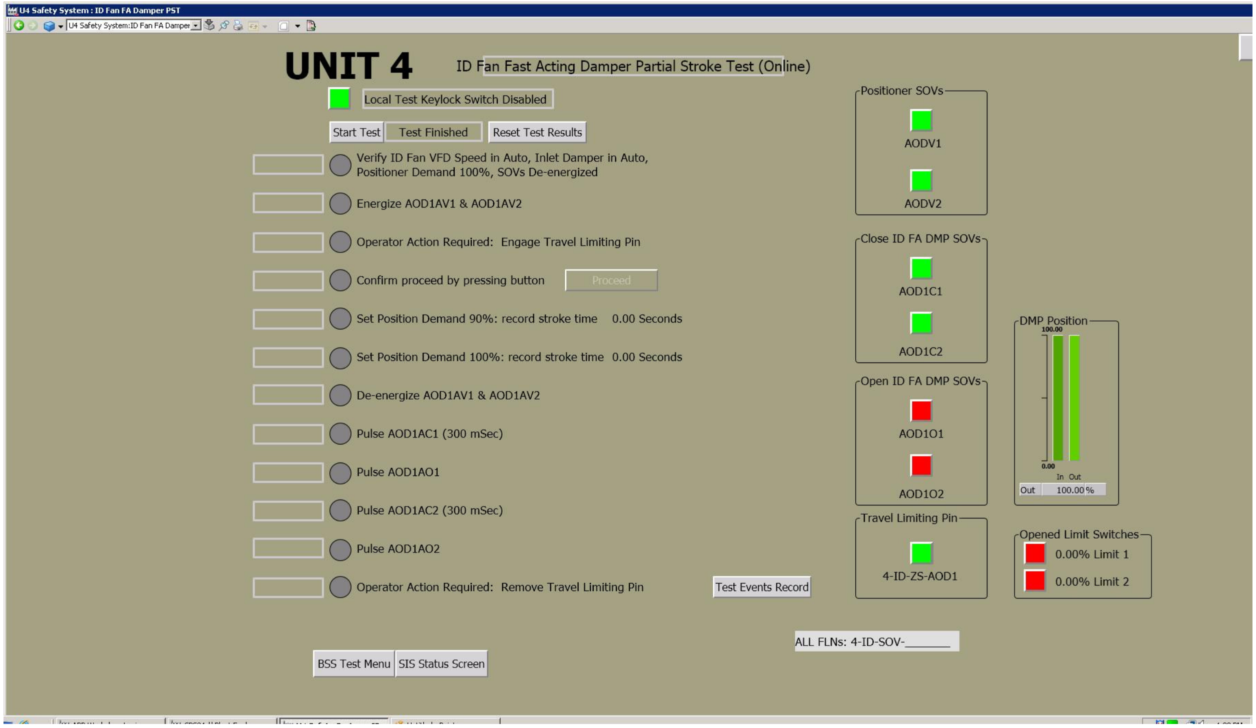
On-Line Tests

- Purge Fan Test
- Purge Fan Inlet Damper Limit Switch Test
- Purge Fan Inlet Damper Solenoid Test
- ID Fan Fast Acting Damper Partial Stroke Test
- Furnace Pressure Transmitter Test

Off-Line Tests

- Purge Fan Test
- Purge Fan Inlet Damper Limit Switch Test
- Purge Fan Inlet Damper Solenoid Test
- ID Fan Fast Acting Damper Full Stroke Test
- ID Fan Breaker Test
- ID Fan Dynamic Braking Test

An example test screen is shown below:



U4 Safety System : ID Fan FA Damper PST

UNIT 4 ID Fan Fast Acting Damper Partial Stroke Test (Online)

🟩 Local Test Keylock Switch Disabled

○ Verify ID Fan VFD Speed in Auto, Inlet Damper in Auto, Positioner Demand 100%, SOVs De-energized

○ Energize AOD1AV1 & AOD1AV2

○ Operator Action Required: Engage Travel Limiting Pin

○ Confirm proceed by pressing button

○ Set Position Demand 90%: record stroke time 0.00 Seconds

○ Set Position Demand 100%: record stroke time 0.00 Seconds

○ De-energize AOD1AV1 & AOD1AV2

○ Pulse AOD1AC1 (300 mSec)

○ Pulse AOD1AO1

○ Pulse AOD1AC2 (300 mSec)

○ Pulse AOD1AO2

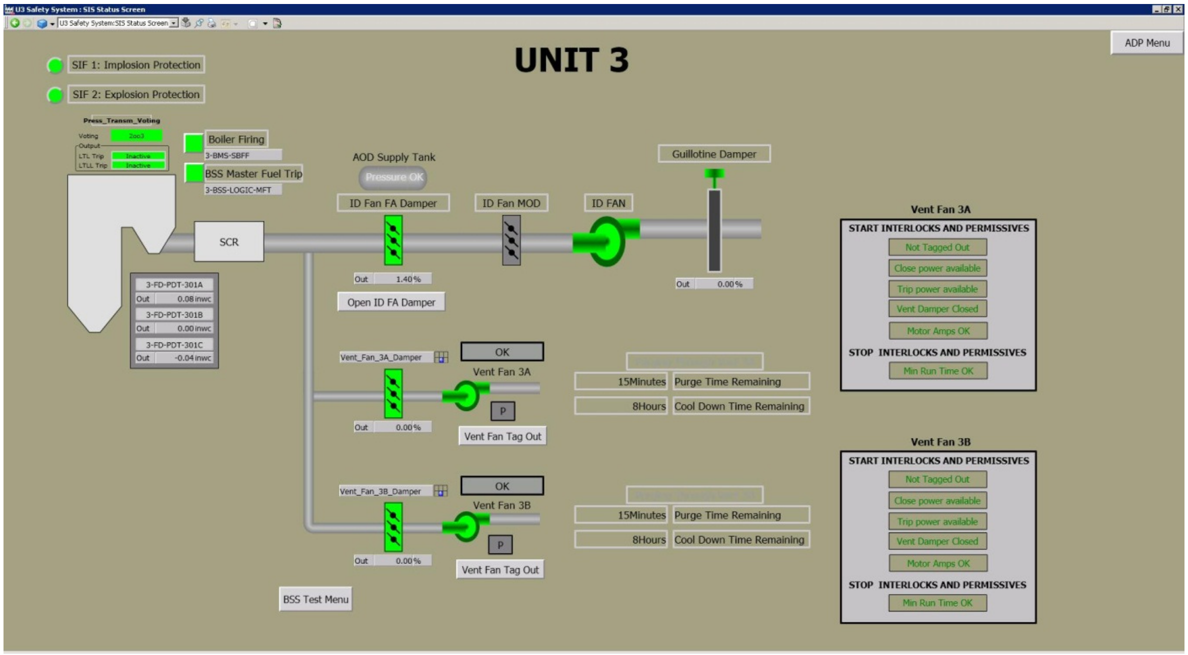
○ Operator Action Required: Remove Travel Limiting Pin

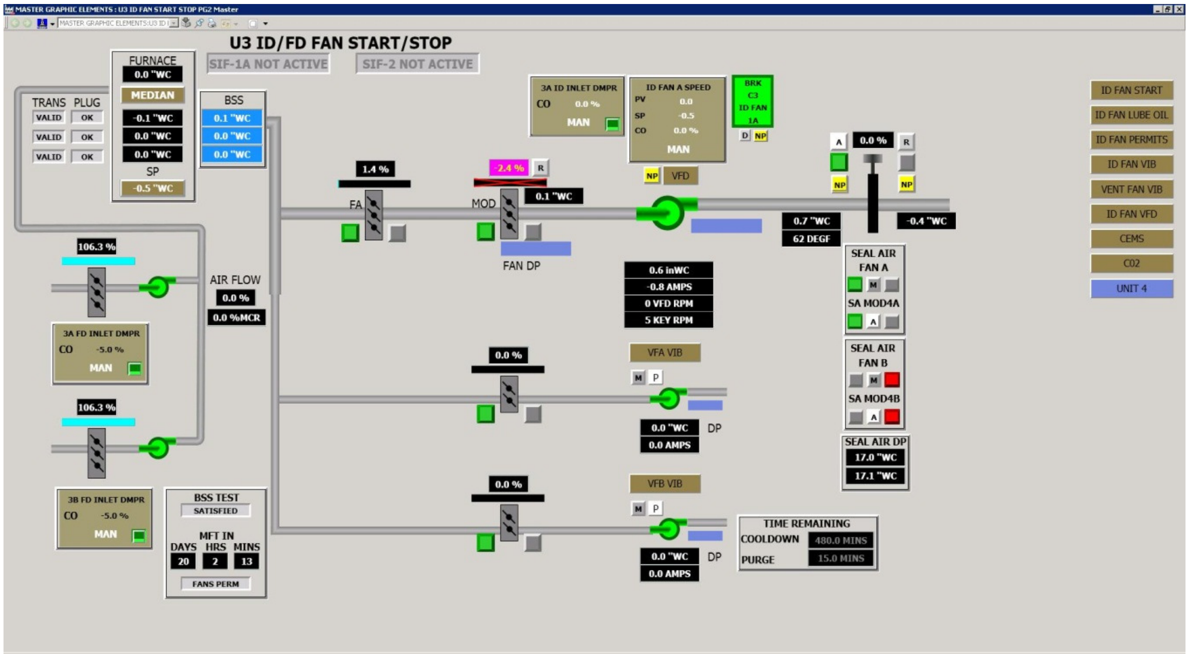
ALL FLNs: 4-ID-SOV-________

Using the energized or de-energized state to perform safety functions was assessed very carefully. Also, the power source for these relays is significant. The consequences of inappropriate operation of the VFD Dynamic Braking Command, VFD Breaker or ID Fast Acting Inlet Damper are potentially dangerous to the process. Each of these was designed to be energize-to-initiate. In the case of the ID Fan Breaker, a relay energizes to trip the breaker. In the case of the VFD Dynamic Braking, a relay energizes to initiate braking. In the case of the ID Fast Acting Inlet Damper, there are two relays and each controls a separate closing solenoid. These too were designed as energize to close the damper. Initially all these relays were supplied by station battery power which is considered to be the most reliable power source in the plant. In the process of writing the safety requirements specification, one subject to evaluate is loss of what happens when house power is lost. In our review, it became apparent that if the plant lost all on site (AC) power, all fans would coast down and the ID Fan Fast Acting Inlet Dampers would still close because they were operated from the station battery. In this special case, it would be best for all the dampers to remain in their last state to allow some natural draft through the furnace, absorber and stack. Based on this analysis, these solenoids were modified to be AC powered. Since all the other dampers on these units were AC powered, the boiler would then be allowed to ventilate through the absorber on a loss of plant power event.

Interfacing the safety system to the BPCS is a significant concern. The safety system we utilized allowed for presentation of data through the BPCS screens since the HMI hardware chosen supported both the DCS and the safety system. The safety system screens were designed to allow for viewing any time but to require a separate safety operator login to perform any control.

Getting the right information on both the BPCS and the boiler safety system screens was accomplished during simulation testing and required a significant degree of operator involvement. Below are copies of the boiler safety system overview screen and the overall BPCS screen.

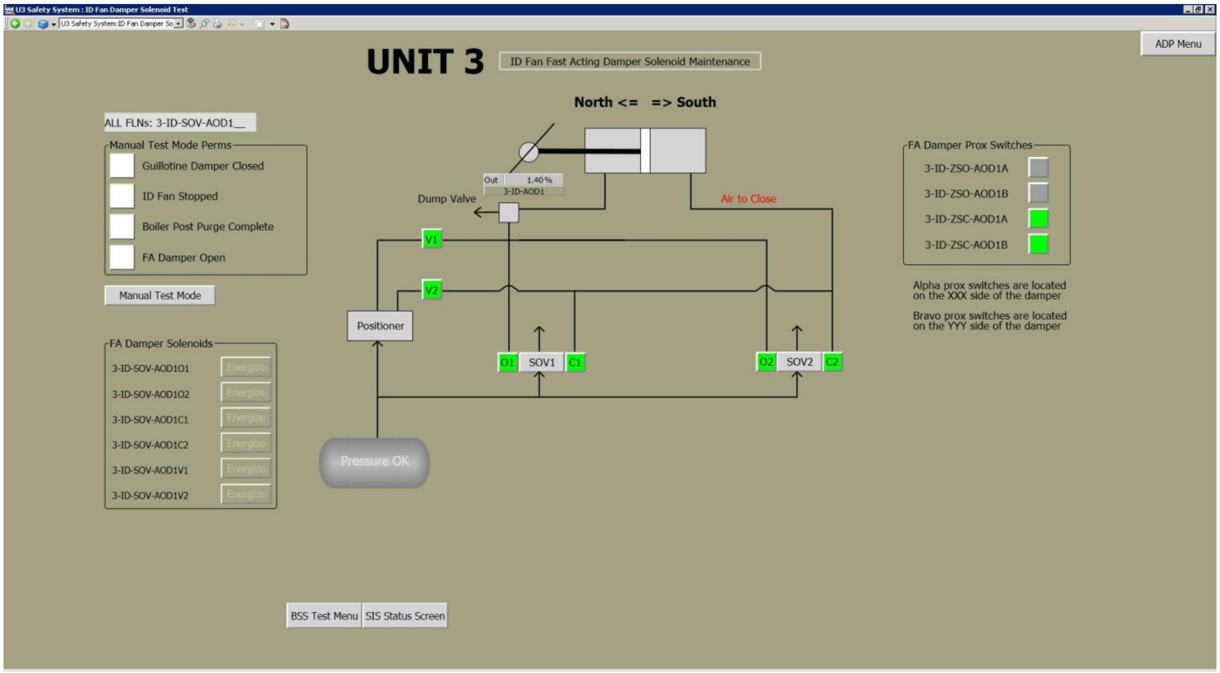




Whenever a SIF (Safety Instrumented Function) is actuated, the boiler will have been tripped already. As a result, the method we determined would be best to reset a SIF was to proceed through the off-line testing required prior to a boiler pre-purge. This would then reset the SIF and allow normal operation.

Regarding overrides, Dominion decided that these would be allowed only when the unit is isolated from the FGD inlet plenum. Special maintenance screens were developed to allow for testing and overriding all solenoid valves. These functions are only allowed if the guillotine damper is closed (isolating the unit from the absorber), the ID Fan is off and a boiler post-purge has been completed.

Below is a copy of one of the safety system maintenance screens.



Alpha prox switches are located on the XXX side of the damper

Bravo prox switches are located on the YYY side of the damper

Safety System Hardware

The boiler safety system was designed using redundant controllers and supervisory modules, redundant communications and redundant I/O. SIL 3 rated controllers and I/O were utilized on all safety functions. SIL 3 rated drives, solenoids, proximity switches and transmitters were supplied. It is important to realize, however, that hardware rating does not translate into system safety system SIL rating. The overall SIL rating of the system is determined by evaluating the PFD for each system function taking into account all equipment including relays, wiring, final devices, sensors, etc.

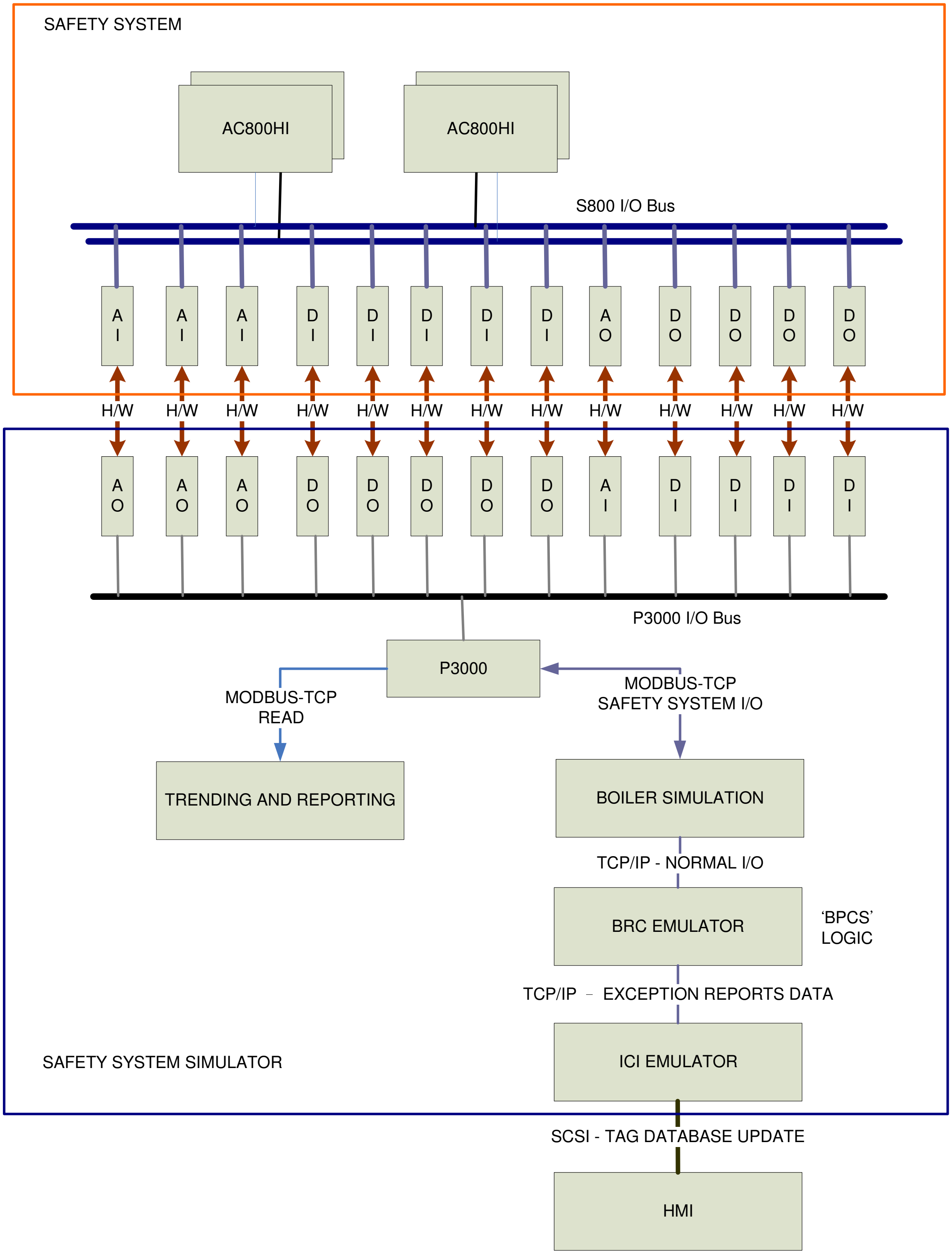
All the safety system I/O is supervised. Digital inputs include resistor networks to monitor the integrity of the wiring out to the field device. Similarly, digital outputs were designed with the driver relay located in the field near the equipment to be operated, not at the safety system I/O cabinet. The digital output modules monitor the status of the wiring to the relays and the relay coil resistance to determine and alarm a failed output relay.

System Development

Dominion was utilizing Microfusion as a system integrator to develop the flue gas desulfurization logic and graphics and for consistency wanted to utilize the same integrator for the safety system design. Dominion brought an ABB safety system engineer into the project to assist with safety logic development. This engineer worked alongside our system integrator for about a month to develop the first unit's logic. Due to his familiarity with both the safety system standards and the hardware platform, this greatly aided our implementation.

Because of the complexity of the safety system and its integration with the BPCS, a full model-based simulation was implemented. The system integrator staged this equipment at his facility to allow for full system testing prior to startup. Dominion attended with engineers, plant technicians and operating personnel.

Microfusion's Think-4^{TM} process simulation software ran on a PC. The DCS hardware was emulated using software developed by Microfusion (shown on this diagram as BRC Emulator). The HMIs were the standard ABB 800xA series hardware/software connected via a SCSI interface developed to emulate ABB's ICI (computer interface), also provided by Microfusion. The ABB 800xA High Integrity safety system was wired to a PLC (shown as P3000) that had a Modbus interface to the model. The diagram shown below provides the modeling system information flow:



There were some issues associated with portions of the system that were not simulated and these had to be worked out. Microfusion was very helpful in providing the missing pieces to make the simulation as complete as it needed to be.

Testing Mandate

The safety rating of this system is only maintained if the testing is performed in accordance with the specified intervals. Because of this, it was decided to implement a testing mandate. All on-line tests must be passed once a month to reset a timer. If the timer rolls past a month without the tests being run and passed, a 72 hour count-down timer is initiated. This indicates very prominently on screen and in the alarm list. At the end of the 72 hour count-down timer, a boiler MFT is initiated. The operators lovingly call this the "Doomsday timer."

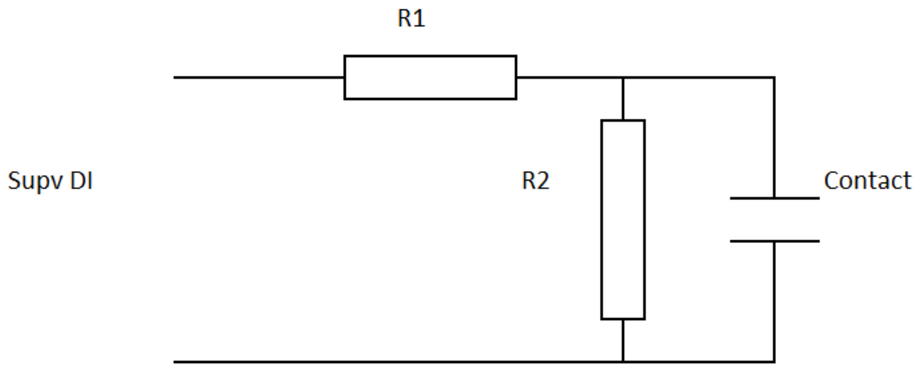
This same methodology is applied for required annual testing.

Similarly, if a critical output channel fails (both I/O cards) this 72 hour timer is initiated.

Finally, if a boiler purge fan is not available, the 72 hour timer is initiated.

Pre-Start Testing

System pre-start testing involved checkout of all system I/O and calibration of all field devices. I/O checking included a detailed test of each input and output point, verifying all the failure modes. For instance, a digital input point has four possible states: closed, open, open-circuit and shorted. Each state needed to be tested and verified on each point.



There are special wiring details for proximity switches and for relays as well. All this information was tabulated in spreadsheets for turnover to plant maintenance personnel.

Due to the unfamiliar nature of this system checkout, Dominion Environmental Projects group required a very detailed checkout schedule identifying every device in the boiler safety and BPCS. This allowed us to very accurately track progress and identify any potential issues that could delay startup.

There were a number of equipment related issues that challenged the checkout schedule. The ID Fan Inlet Fast Acting Dampers were provided with a connecting link (attaching dampers on both fan inlets) that were inadequate for the high speed operation of these dampers. These needed to be substantially beefed up. Tubing and pneumatic components were undersized as well. Resolving these issues delayed checkout substantially, but eventually the modifications resulted in reliable damper operation in under 4 seconds.

The VFD dynamic braking setup was another hurdle to jump. This proved to be beyond the knowledge of the first field service engineer provided by the manufacturer. A second, more knowledgeable engineer was able to set this up correctly and the Unit 4 and 5 fans were verified to brake in under 10 seconds as specified. Unit 3 fans proved to be another story. After repeated attempts, it became clear that these fans could never achieve the desired braking requested in our design. This resulted in some late design changes to the safety system for that unit and a delayed startup.

Ultimately, Units 4 and 5 were started on schedule and Unit 3 was delayed due to the ID Fan VFD issues.

System Startup

Unit 5 was the first unit to start. A Site Acceptance Test Plan was developed by the Dominion Engineering group. This involved performing all the off-line testing and the new boiler pre-purge permissives. Testing was performed on maintenance switches for furnace pressure transmitters to allow for on-line calibration. Hard-wired pressure switch interlocks were tested. Fans were started and furnace pressure tuning was completed. A boiler purge was completed and a loss of lube oil event was simulated on each ID Fan. On-line tests were performed and confirmed. A SIF-1 event (extremely low furnace pressure) was initiated and all actions confirmed. Finally, a SIF-2 event was initiated (loss of both ID Fans) and all actions confirmed. This involved about 4 days of testing with fans running up to full load airflow. As far as possible, testing was designed to emulate the real process events. Unit 5 was then released to operations for startup.

Unit 4 was tested similarly, following the Unit 5 outage. The only salient differences were that there was only one ID Fan and Two Purge Fans. The CO_2 system was tested in conjunction with this but this system was independent of the boiler safety system.

Unit 3 was delayed due to an early VFD transformer failure and due to the inadequate braking capability of the VFD. Dominion evaluated changing to a different style of VFD, stiffening the boiler and other modeling based alternatives to resolving the issues with Unit 3. Through a revision to existing logic and some boiler stiffening, this was achieved in about 4 months.

Operation

In operation, some issues developed due to the monthly and annual timing circuits. These were not fully tested during the factory simulation due to scheduling. These logics required changes after the first few months of operation.

There was also an issue with the safety controller firmware that affected its ability to determine I/O status. This problem caused intermittent I/O card failures and this problem resulted in a unit trip. Engineering worked with the safety system vendor, ABB, to resolve this issue.

Final SIL Validation

After startup, Dominion sought to validate the design utilizing the same consultant that performed the initial PHA work. Once again, the team of engineers, corporate loss prevention, operations and technical support was assembled. The implemented logic was evaluated using the LOPA and Fault Tree analyses. This review found that there were some weaknesses in the system that would prevent it from meeting the SIL targets defined. Special operating procedures were put into place to carry the units until these changes could be made.

- Test procedures were written, added and tested for ID Fan VFD Breaker Testing and Dynamic Braking. These were not originally included.
- Since the VFD is potentially a cause for SIF-2, alarm response procedures were requested from the supplier to give the operator specific guidance. Proper response to these alarms could prevent a SIF-2 event.
- ID Fan Fast Acting Damper close solenoids were rewired such that a close command always overrides an open command.
- Hard-wired directional blocking was added to the FD Fan Inlet Damper Drives. Based on a pair of pressure switches, if furnace pressure is too low, the close circuit to the Beck drive motor is broken. This provides a hard-wired backup to an identical function that resides in the BPCS. This was done to eliminate one of the possible initiating causes of furnace implosion.
- Modify logic for FD Fan statuses to be based on breaker status and amps. This is intended to prevent an ID Fan trip that could be caused by a faulty indication that the FD Fans are off.

Lessons Learned

When someone mentions the words “safety system,” SIL or PHA, multiply all reasonable man-hour estimates by 4.

Make overview screens for the safety system and the BPCS as similar as possible. Differences in layout cause operator confusion.

Write the best possible Safety Requirements Specification.

Train I&E Technicians on the safety system equipment prior to the Factory Acceptance Test.

Allow time in the engineering cycle for a final SIF Review prior to construction.