

# Integration of Complex Sequences using DeltaV

2007 AIChE Spring National Meeting

## Authors

Dean Taggart, P.Eng, CFSE  
Emerson Process Management  
Hydrocarbon and Energy Industry Center  
Calgary, AB, Canada

Richard Maisonneuve, P.Eng  
OPTI Canada Inc  
Calgary, AB, Canada

John Kingston, P.Eng  
Spartan Controls Ltd.  
Edmonton, AB, Canada

George Cushon, P.Eng  
OPTI Canada Inc  
Calgary, AB, Canada

Stephen Krause, CET  
Emerson Process Management  
Hydrocarbon and Energy Industry Center  
Calgary, AB, Canada

## Acknowledgements

Robert Schouwenaar  
Shell Global Solutions Inc.  
Amsterdam, Netherlands

## Abstract

Companies have often struggled with the implementation of complex sequences involving tight integration of the SIS and DCS. Implementation often proved difficult due to the independent nature of SIS, which is problematic when communication between the SIS and DCS is important.

With the release of DeltaV SIS, those issues are no longer a concern. DeltaV SIS along with DeltaV BPCS presents options not available before.

For a very complex application like startup and shutdown of an oilsands gasification process, DeltaV BPCS and DeltaV SIS are an excellent fit. With the State Transition Diagram function blocks now available with DeltaV SIS, and with the proper implementation methodology, implementation can be done in a logical, efficient manner. With PlantWeb integration, the creation of HMI displays as well as interaction with the highly complex DCS control are greatly simplified.

This paper describes the design issues for integration of the safety, control and operator functions in this new architecture. Technical issues such as the use of equipment (position transmitters, DVC's) and DCS/SIS interaction are discussed, as well as the importance of the implementation framework, which is the heart of the design.

## Introduction

There are many complex processes that involve both a SIS and a DCS (BPCS), and some industries see this more often than others. These complex processes pose various challenges that must be overcome. This paper will discuss three key areas:

- Process and Safety Requirements, with their various
- Technical Concerns, which when dealt with properly, lead to an
- Implementation Framework

## Process and Safety Requirements

### Factors to Consider in Determining the Degree of Automation for a Process

One of the key questions to be asked when designing the automation system for a process is “Can the requirements be met by an operating procedure, or is it necessary to embed the process and safety requirements in the automation system?” There are a number of factors to consider when determining what the “right” amount of automation is for a particular process:

1. Process Complexity
2. Integration and interaction needs
3. Process control requirements: the “size” of the safe operating envelope
4. Safety function requirements
5. Operating experience and knowledge
6. Economic optimization requirements: the “size” of the optimal economic envelope

The impact of these factors on the degree of automation will be discussed in the following sections using Figure 1, Generic Process States. Every process will have at least one state each for maintaining, preparing, starting, running or shutting down the process. Typically, the requirements for the Run and Shutdown states are embedded in the automation system and the requirements for the other states are largely met by operating procedures. An example of a simple unit operation within a larger process will be used to illustrate the impact of the factors listed above. The simple unit operation consists of a centrifugal pump, driven by a small electric motor, with a control valve in the discharge line used to control the level in a vessel.

### Process Complexity

Assume that the pump is down for maintenance to repair the impellor, and the process is in the Maintain state. The safety requirements for this state are a function of the process fluid, system pressure, temperature, and other various factors. The automation requirements will be minimal for low pressure, low temperature systems with an innocuous fluid. Most often, the safety system does not act in this state.

After the maintenance work is complete, the pump must be prepared for startup. A typical preparation activity for a centrifugal pump is to check its rotation by “bumping” the electric motor. This requirement is quite simple and is very rarely automated. Hence, it is handled by an operating or maintenance procedure.

Let’s now assume that instead of a small centrifugal pump with an electric motor, the process has a large centrifugal pump with its own utilities driven by a large steam turbine. This increases the process complexity since the pump and turbine will have utility systems that must be prepared for startup. Typical preparation activities include re-circulating the lube oil, warming up the steam feed lines, and checking lube oil cooler operation. Each of these activities needs to be reviewed to determine if embedding the requirements in the automation system is beneficial, for example to prevent equipment damage.

Once the pump and turbine are prepared, they are now ready for startup. For large turbines and pumps, there are a series of actions that must be executed in the correct order to prevent equipment damage. These actions are executed in the Startup state and culminate in reaching the Run state, if all permissives are met and all the actions are executed correctly. Otherwise, the automation system will either hold or initiate a shutdown. The shutdown requirements may also require a series of actions to safely shutdown the process. For the large centrifugal pump example, there may be a post lube requirement on spin down to prevent damage to the bearings.

In the Run state, the level controller becomes active. Typically, it must maintain the level at least above the level required to prevent pump cavitation. If this is not met, then a shutdown is initiated. However, the actions required may not be the same as a shutdown from the Startup state. For example, in a shutdown from the Run state, the turbine may be kept running at a minimum speed.

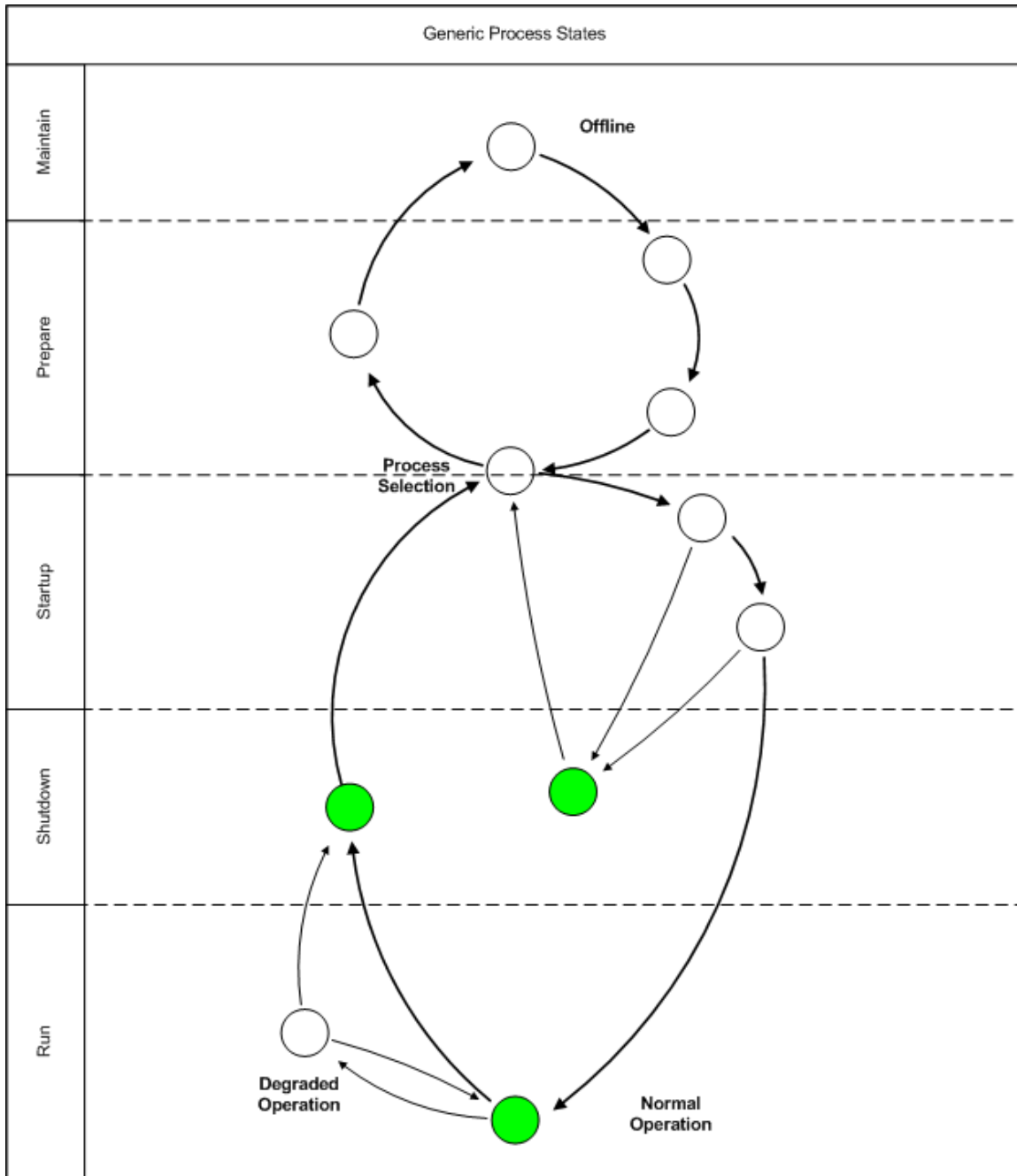


Figure 1: Generic Process States

**Integration and Interaction**

For a stand alone process unit, such as an oil battery for truck offloading and oil/water separation, there will be limited interaction or integration requirements. There is a low probability that a disturbance in the oil battery will have a significant impact on the pipeline operation. However, the relationships between process units in large processing facilities such as a refinery, petrochemical facility, or oilsand upgrader need to be examined for their integration and interaction requirements. A facility designed with

intermediate tankage between the process units has limited interaction between the units, and a problem in one unit can be handled procedurally without propagating the problem to other units.

That said, most facilities being built today have limited intermediate tankage (if at all), yet have interdependency for feed streams and utilities. This means that a disturbance in one can have a negative impact on overall performance unless they are addressed in a timely manner. The limited time available for operator action may require that the remedial actions are automated; otherwise, the problem propagates through several process units with potential multiple unit trips, thus reducing availability.

### **Process Control Requirements - “Size” of the Safe Operating Envelope**

The safe operating envelope of a process is a subset of all possible operating conditions that are considered to be safe. The safe operating envelope is determined during the process design phase using risk assessment and analysis tools such as HAZOP, LOPA, etc. Some processes have a large envelope and when a disturbance arises, the process stays within the safe envelope prior to remedial action. The new set of conditions is not desirable but still within the safe region. Thus the operator has time to assess the impact and determine the best course of action.

For processes with a small safe operating envelope, a disturbance can drive the process towards the unsafe region - particularly if the disturbance has fast dynamics. The process will cross into the unsafe region if not corrected quickly and must be shutdown by the safety system or dealt with by other layers of protection, such as relief devices. In these cases, the process control requirements should include the ability to reject disturbances and not require operator intervention as a first response.

### **Safety Function Requirements and Design Basis**

One of the main objectives of a safety system is to safely shutdown the process if it moves outside of the safe operating envelope. To that end, the detection of the unsafe condition and the subsequent actions required will have an impact on the degree of automation. For the simple centrifugal pump example, the detection of a low level in the vessel and the actions to shutdown the pump are straight forward. More complex processes can require sophisticated shutdown sequences that are dependent on the current state of the process.

The design basis for the safety requirements also impacts the degree of automation. The safety requirements may consist of several different layers of protection. For example, sometimes operator intervention is all that is required, or a safety instrumented system is required to intervene. These are protection layers. There may also be relief valves or rupture disks, dikes, walls, and emergency response systems. These are mitigation layers. Depending on the process and the design, there may be no requirements for a safety instrumented system.

In some cases the PHA/LOPA/Risk Analysis may indicate that the engineering design and the existing layers of protection are not enough, and a safety instrumented system is required. Depending on how much further risk reduction is needed, a safety integrity level (SIL) target is established (SIL 1 up to SIL 4). Additional sensors, logic solvers, and end devices are *added* to the engineering design and constitute a safety instrumented system, composed of one or more safety instrumented functions (SIFs).

In the case of the centrifugal pump example, there may be a need for a SIF to trip the pump as well as force the control valve closed (with a solenoid on the instrument air supply). It may also require a block valve after the control valve. The SIS would have an independent set of sensors in the vessel to measure level. In this way, if the process control system fails to control the level, either due to failed level sensors, issues with the control valve, or inability to control the pump, the SIS would take protective action.

IEC standards (IEC 61508 and 61511) and ANSI/ISA standards (S84.01) are both performance based standards governing SIS for the process industry. The operating company is responsible for setting their acceptable risk levels, and ensuring that the risk is reduced to those levels. This may require a SIS, or may not. The important thing is that these are not prescriptive standards; hence the owner is able to do what is most appropriate for the situation.

### **Operating Experience and Knowledge**

For processes where the technology is well established, the pool of technical staff available to run the process tends to be large (barring any local market conditions). As such, there is less of a driver to automate the required actions since they can be effectively executed by a well-trained and experienced operations team.

In cases where new technology is being applied, the process is new to an industry segment, or the job market is fluid, consideration should be given to embedding more of the requirements into the automation system to ensure that the correct remedial actions are executed based on the given situation. Further, operating knowledge is captured in the automation system and, as such, an operating company is less impacted by a tight job market.

### **Economic Optimization Requirements - “Size” of the Optimal Economic Envelope**

As stated above, the safe operating envelope is a subset of all possible operating conditions that are considered to be safe. Within this envelope there is further subset of operating conditions that achieves an optimum economic result. The desired result is usually stated as an objective function such as maximize profit or minimize cost, etc. Note that the optimum economic envelope may move depending on economic conditions such as price of finished products and raw material costs.

Typically, an optimizer application solves the objective function and determines a set of conditions that the process should operate at. The changes are made automatically or

operating instructions are provided to the operator. The method used to make the changes will affect the degree of automation required. Note that for the optimizer to be effective, the underlying regulatory control must be designed and function well.

## Gasification

### Process Description

In the previous section we discussed the factors affecting the degree of automation in a general way. In this section, we discuss these factors in relation to the Shell Gasification Process (SGP) for the Long Lake bitumen and upgrading project now under construction by OPTI Canada Inc. and Nexen Inc. It is the first application of large scale gasification in Canada, and the first implementation of a gasification project in conjunction with a heavy oil recovery and upgrading project (Arnold et al. 2002).

Figure 2 below shows the integration of the three main components of the Long Lake Integrated Upgrader: OrCrude primary upgrading, liquids asphaltene gasification, and hydrocracking of the OrCrude product. A key advantage of the Long Lake Upgrader configuration is the integration of an asphaltene gasification unit into the upgrader system to provide hydrogen to the hydrocracker and fuel for power and steam generation. The energy balance of the project eliminates virtually all of natural gas cost exposure, which results in an operating cost advantage of about 50% over currently configured operations.

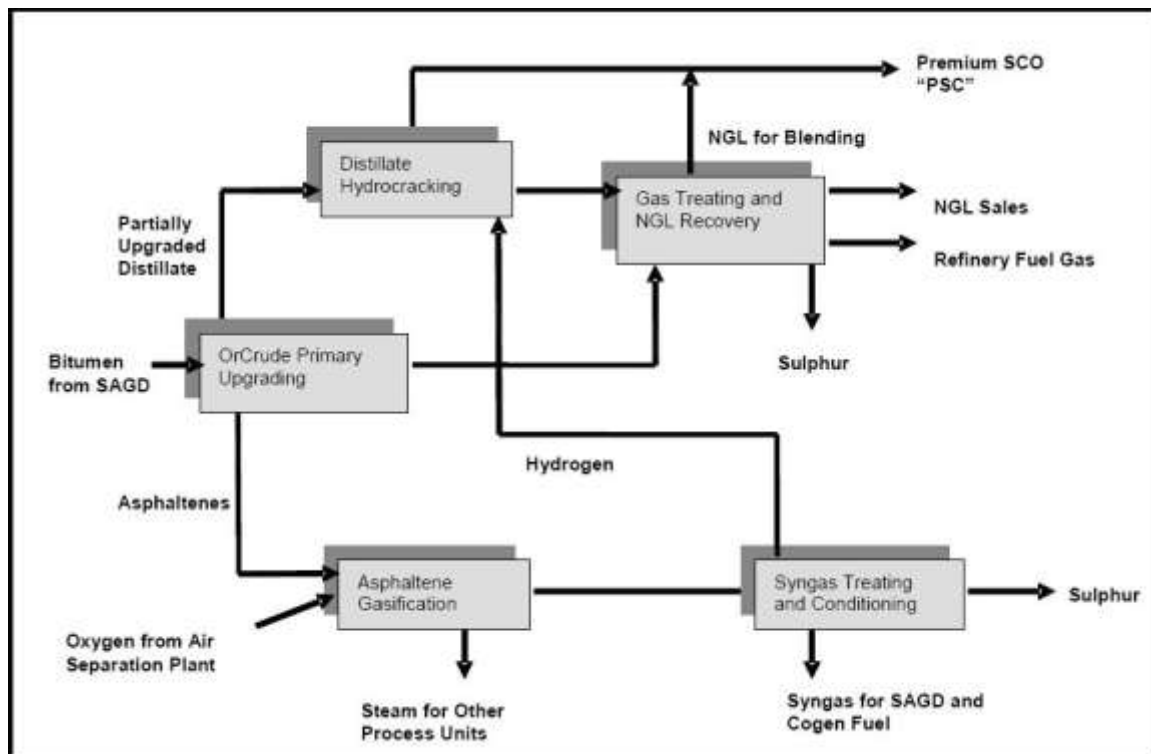


Figure 2: Long Lake Integrated Upgrader

Figure 3 is a schematic of the Shell gasification process for the Long Lake Upgrader. The non catalytic partial oxidation of the asphaltenes takes place in a refractory lined reactor that is fitted with a specially designed burner. The high pressure oxygen, supplied by the air separation unit (ASU), is preheated and mixed with steam prior to being fed to the burner. The Long Lake Project uses four 1033 tonne/day (each) gasification reactors, normally operating with all four running at less than 100% capacity, with the feed rate following the asphaltene production rate from the OrCrude unit.

The burner and reactor geometry are so designed that this mixture of oxygen and steam is intimately mixed with the preheated asphaltene. The burner is a co-annular design using blast atomizing. The product of the partial oxidation reaction is a raw synthesis gas at a temperature of about 1300°C that contains particles of residual carbon and ash. Primary heat recovery takes place in a syngas cooler, a Shell proprietary design, generating high pressure steam cooling the syngas to about 340°C. Secondary heat recovery takes place in a boiler feed water economizer immediately downstream of the syngas cooler.

The reactor outlet syngas contains a small amount of soot in the form of carbon particles that are removed from the gas together, along with the ash, in a two-stage water wash: first quenching with water followed by scrubbing with water. The resulting carbon/water slurry is filtered to recover the process condensate which is recycled to the water wash circuit.

The product syngas leaves the scrubber with a temperature of about 40°C and is treated in a single gas purification system. The treated syngas is fed to a Pressure Swing Adsorption (PSA) unit for hydrogen recovery, with the recovered hydrogen being sent to the Hydrocracker unit. The high pressure tail gas from the PSA flows directly to users: steam generators and two gas turbine generators for power generation in a cogeneration system.

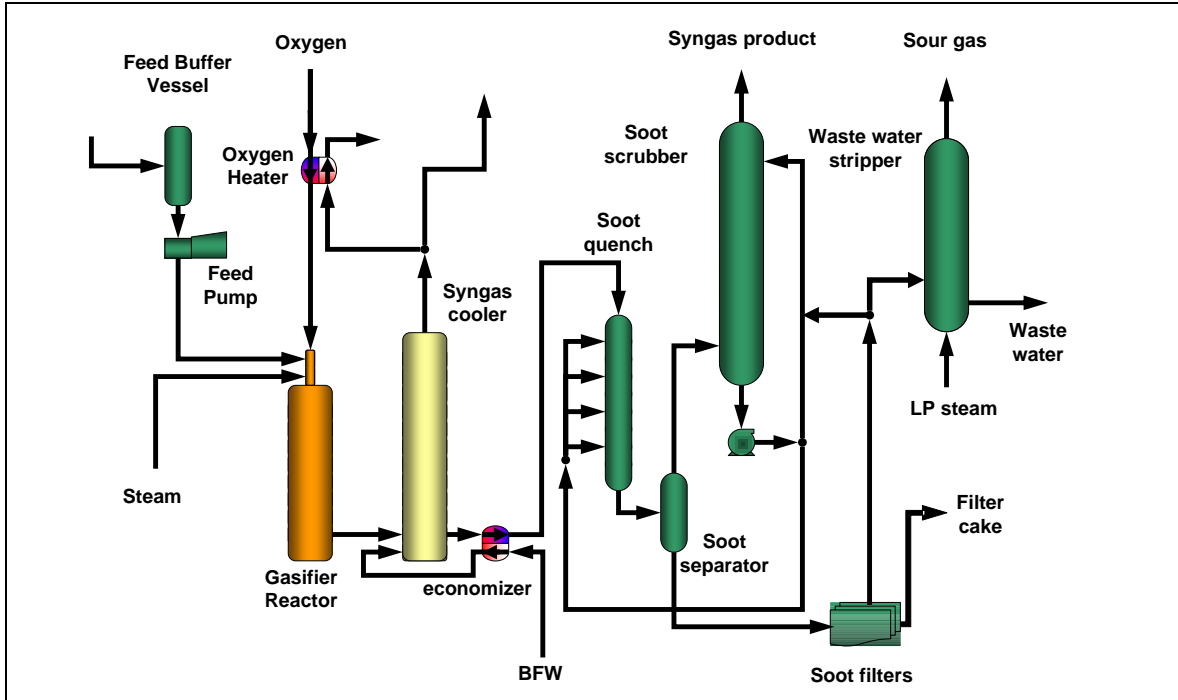


Figure 3: Shell Gasification Process

Factor affecting Degree of Automation	Low	Medium	High
Process Complexity			X
Integration and Interaction Needs			X
Process Control Requirements – Safe Operating Envelope		X	
Safety Function Requirements and Design basis			X
Economic Optimization Requirements – optimal economic envelope	X		
Operator Knowledge and Experience			X

Table 1: Gasification Automation Score Card

### Process Complexity

The partial oxidation of the asphaltenes, waste heat recovery, carbon removal, and syngas treatment processes are not complex processes if one is focused on the requirements for the Normal Operation state (see Figure 1). However, the preparation, startup, and shutdown states for the gasification system add complexity. In the preparation states there are several activities that are completed with the reactor at elevated temperature (around 800°C) with all streams to the reactor isolated. For example, inspection of the burner using an endoscope is done with the reactor opened up but under a slight vacuum. During this time, some safety functions are suppressed in order to ensure the operators can complete the tasks safely without a major trip occurring (a case in which the attempt to move to the safe state actually causes a hazardous situation).

The shutdown sequence is quite complex. The actions must be executed in the correct order or mechanical damage will result to either the burner, refractory lining, or to the syngas cooler. There are a number of abnormal conditions that must be dealt with during the shutdown using a combination of operating procedures and automated actions.

Finally, there are actions that must always be executed *independently* of the state of the process to prevent mechanical damage of the equipment. These actions must be coordinated with the state dependent (regularly performed) actions. Therefore, the gasification process scores High on process complexity.

### **Integration and Interaction Needs**

As presented above, gasification is one of the three main components of the Long Lake Integrated Upgrader. The gasifier is fed from the OrCrude unit with limited buffering between the units. The gasification feed rate must be adjusted to maintain a suitable inventory in the feed vessel. However, the allowable feed ramp rate is limited and large upsets may require changes in the OrCrude unit to resolve.

The hydrogen produced by the gasification unit is used by the Hydrocracking unit to upgrade the OrCrude product to Premium Synthetic Crude. There is no intermediate storage and the PSA unit requires a minimum feed rate to meet product specifications.

Therefore, the gasification process scores High on Integration and Interaction Needs.

### **Process Control Requirements – “Size” of the Safe Operating Envelope**

In the Normal Operation state, the partial oxidation of the asphaltene is controlled by adjusting the oxygen/oil ratio instead of reactor temperature. This is required because thermocouples cannot survive in the harsh conditions within the reactor for long periods of time, and they do not provide a reliable enough measurement for direct control of the reactor temperature. A small change in oxygen/oil ratio has a large impact on the reactor temperature, which will affect the degree of oxidation. Too high a temperature results in exceeding the mechanical design temperatures; too low a temperature results in high soot make.

However, most of the other process control requirements are straightforward and are somewhat forgiving when in the Normal Operation state. There are some challenges for stable control in the transition from startup conditions at ambient pressure to the normal operating pressure of about 65 bar. Therefore, the gasification process scores a Medium for Process Control requirements.

### **Safety Function Requirements**

The safety function requirements for the gasification process are very complex. The requirements are centered on preventing damage to the burner, reactor, and syngas

cooler, as well as operator safety. The required actions change depending on the state of the process. Typically, the safety function requirements define the process shutdown requirements once an unsafe condition is detected. For the gasification process, the safety function requirements extend into the startup states where a sequence of actions must be executed to prevent mechanical damage. Typically there is a clear distinction between process control function and safety function. This is not case for the gasification process. Therefore, the coordination of actions between the SIS and the BPCS must be examined closely. Finally, the required shutdown actions are dependent on the state of the process in which the trip occurred, and must be executed in a specific order and must take into account any abnormal conditions that may have occurred, such as loss of HP steam. Therefore, the gasification process scores High for safety function requirements.

### **Economic Optimization Requirements**

Every process has an optimal set of operating conditions that produces a desired economic result. However, for the gasification process there is only a small economic advantage between an operating point within the safe operating envelope and the economic optimum operating point. Therefore, there is little incentive for economic optimization and the gasification process scores Low for this factor.

### **Operating Experience and Knowledge**

As stated above, the Long Lake project is the first application of large scale gasification in Canada and the first implementation of a gasification project in conjunction with a heavy oil recovery and upgrading project. Further, the gasification process with its structured startup and shutdown requirements is not common for refining and upgrading facilities in Alberta. Conversely, the current skill set of operators in the Alberta market is broad enough that experience from other industries and processes can be applied in conjunction with good operator training for the gasification process. Taking this into account, the gasification process still scores High for Operator Experience and Knowledge.

## Technical Concerns

### SIS/BPCS

#### **What should be in the BPCS or the SIS**

As discussed earlier, there are both protection and mitigation layers of protection for any process design. Normally the process is designed in a Front End Engineering Design (FEED) phase, where vessels, pumps, piping, and instrumentation are proposed. The process goes through a HAZOP process, with the intent of identifying hazards. As these are considered, either through a PHA, LOPA, or Risk Analysis, SIL targets are determined and requirements for SIS are established.

One would, under normal circumstances, expect that all issues relating to the startup of a process would be in the realm of normal process control. One would also assume the stopping of that process to be normal process control. In some cases, a SIS might be called on to “trip” the process, which is a simplistic way of saying return the process to a safe state. It is not common to find the SIS involved in startup sequences or stopping sequences.

However, in cases that deal with burners, especially involving vessels under high pressure and temperature, you start to see SIS involved in the startup sequence. This is because if the feeds are not established properly, the startup itself can cause an explosion. For example, a burner management system is almost always a SIS, and the startup is governed by the SIS.

In a BMS, the shutdown is a simple one – generally, close off the feeds (natural gas and fuel gas) and the burner will go out. But in a process like a gasification reactor, you cannot simply block in the reactor and leave it that way. The vessel is under high pressure and high temperature. The asphaltene feed will, if not evacuated quickly, harden and plug up the feed lines. It must be depressured and cooled down in a manner that will not damage the equipment. Even the emergency depressurization must be controlled. Finally, there are critical requirements for cooling the burner, and a loss of boiler feed water or HP Steam during a shutdown would cause additional hazards, so the shutdown sequence must be “adjusted”.

All of these things result in a simple conclusion: almost all of the startup and shutdown sequence must be performed within the SIS. It would be possible to split these sequences apart and allocate some to the SIS and some to the BPCS; however this would make the configuration even more complex.

Fortunately, a sequence is within the capability of a SIS. There are certain things that don't really belong in a SIS, for example, intense and complex mathematical calculations. These are best left to a BPCS (and it is quite difficult to find a SIF that depends on a complex mathematical calculation).

In the past there was a concern that SIS I/O was more expensive than BPCS I/O, due mostly to the hardware redundancy and diagnostics that must be built into a SIS logic solver. However, these days there are several SIS that are more cost effective, and operating companies are realizing that excessive redundancy is not always required (an important aspect of SIS design is cost-benefit analysis – something often neglected in the past).

### **Communications**

How the SIS and BPCS will communicate is a very important topic. There are essentially three different methods of communication: OPC communication, serial communication, and proprietary communication.

With OPC (OLE for Process Control) communication, an OPC server is set up to serve data to another system. In this type of setup, usually both systems will have an OPC server. Therefore in order to have two servers talk properly with each other, you also need to setup an OPC mirror. Finally, if you want a redundant solution, this becomes increasingly complicated.

With OPC, there is typically a high amount of integration time doing data mapping. The architecture is complex, and it can be slow (in the sense that the data retrieval may be slow, and it can also use up endless resources).

Serial communication, which is normally done using a protocol like Modbus, has similar issues. There is a large amount of integration time for data mapping. Redundant solutions can also be complicated. In all fairness, recent advances remove some of these issues. For example, there are now VIM Network Gateways for DeltaV systems that can be easily setup as redundant gateways. With both OPC and serial communication, diagnostic information is crucial, and the engineer will likely have to build their own diagnostics and watchdogs.

With proprietary communication, it is likely that more diagnostic information is built into the protocol. Several vendors now supply this, and the DeltaV / DeltaV SIS is one such system. With proprietary communications, a system is faster and generally more reliable. It has better diagnostic information and better fault handling. Finally, it has much faster “integration” time since there is no data mapping; a browse window is used to configure links between data in the BPCS and SIS.

Regardless of the solution chosen, there is one very important issue that cannot be forgotten. No matter what happens in the BPCS, failure of the BPCS or the communication link can not adversely affect the proper function of the SIS. Only non safety critical data should be passed from the BPCS to the SIS, and the SIFs can never depend on any data supplied by the BPCS.

### **Where the sequence belongs**

For something as complicated as the startup and shutdown of a gasifier, the sequence is very important. As mentioned already, the sequence could be split apart into SIS and BPCS components, or the entire sequence could be put into the SIS.

While this exercise would be difficult, there is also an underlying concern that prevents us from separating the sequence. In order to work properly the BPCS and SIS would have to have “parallel” sequences which would need to be synchronized very tightly with each other. In the event that communication was lost during a startup or shutdown, each would have to execute separate and parallel actions. Since the actions may need to be modified based on process conditions, this adds even more complexity.

If the sequence is placed fully in the SIS, configuration is simpler. Under normal circumstances, the SIS runs the sequence, can override the BPCS when required, and can examine the health of the BPCS. The BPCS only performs process control, listens to the SIS for overrides, and can examine the health of the SIS. If communications is lost, the SIS can take the appropriate action (perhaps abort a startup, execute a shutdown, or may do nothing at all if in normal operation). In this case the BPCS may continue to execute process control on some loops, and for others they may automatically be set to override or manual mode. The flexibility is there, and there is little concern over loss of communication.

### **HMI Integration**

HMI integration is a key to a successful system. The HMI should clearly indicate to the operator, through visual cues and special screens, what is in the SIS versus what is in the BPCS. Even though there is a clear difference between what is SIS and BPCS, the operator should be able to interact with them both in the same ways.

In addition, the safety standards have some additional requirements for an HMI. For one thing, any change made by an operator to an element of the SIS (a bypass, reset, or other similar command) must have a repeat confirmation step. This is to prevent an operator from inadvertently causing a hazard. Also, when an initiating event, intermediate event, or incident occurs (see CPQRA for definitions), the operator should be made aware and should have an easy means of evaluating and acting, with minimum searching and minimum “button clicks” and navigation.

Above all else, the Human Machine Interface must be easy to use.

### **Safety Requirements**

#### **Availability vs Reliability**

In order to properly discuss this, it is first important to come to a full understanding of availability and reliability. For whatever reason, the meanings of the words availability and reliability have been contentious in the past.

The simplest way to consider reliability and availability is this: the reliability is the measure of a systems ability to do the right thing when needed, and availability is the probability that when a system is needed it will be functioning.

In mathematical terms, reliability is the *probability of success during an interval of time*. Reliability (R) is a function of failure rate and the time interval.

$$R = e^{-\lambda t} \quad (1)$$

where    R     = Reliability  
            $\lambda$     = constant failure rate  
           t        = time interval

It is also important to consider that there is no failure and repair during the interval.

Availability is the *probability of success at a moment in time*. Availability (A) is a function of the failure rate and the repair rate. Considering a single failure mode, with constant failure rate  $\lambda$  and a constant repair rate  $\mu$

$$A = \text{MTTF} / (\text{MTTF} + \text{MTTR}) \quad (2)$$

where    A     = Availability  
           MTTF =  $1/\lambda$   
           MTTR =  $1/\mu$

When applied to gasification, it is apparent that both reliability and availability must be maximized. The gasification reaction poses some interesting problems. The gasification burner itself has a limited lifespan due to the harsh conditions within which it must operate. Damage to the refractory must be avoided by adhering to strict process conditions during the startup and shutdown sequences. The reactor operates at high temperatures, and requires special thermocouples that can operate at those high temperatures. It is very common to have thermocouple failures during the startup sequence. Some operations, like thermocouple replacement and endoscope inspection, need to be done when the process is warm. Finally, during the startup sequence there comes a temperature when an auxiliary burner must be replaced by a dummy burner, since it can no longer withstand the higher temperatures. Given all these issues and the time to get the reactor started up, once running it needs to be kept running safely for as long as possible.

To assist with the availability, there are a few things that need to be done. All the logic solvers must be redundant, and all communications must be redundant. What this provides is the ability to repair the systems without having the systems in a non functioning state. A loss of communications should not automatically cause a shutdown; this should be governed by the state the process is in. For example, it is safe to operate in normal mode with a loss of communication, but it would be dangerous to continue with a startup sequence in such a case. A bad process variable does not in all cases need to

cause an immediate trip; in some cases it is better to leave this decision up to the operator. An obvious example is the thermocouple case, since the operator actually expects some thermocouples to fail during startup. To help availability, the operator is given more decision making responsibility.

To assist with reliability, better diagnostics are needed to reduce the probability of dangerous, undetected failures. HART devices are used as often as possible, to provide the operators with additional diagnostic information (and possibly find problems with devices before they occur). The preference is to use failsafe position transmitters, since they have a much higher reliability than other solutions. In every possible instance deviation alarms are set up between not only redundant SIS sensors but also between SIS and BPCS sensors. This type of comparison can provide approximately 95% diagnostic coverage factor, which is a huge benefit. Valves with Digital Valve Controllers (DVC's) capable of partial stroke testing should be used whenever possible, as partial stroke testing can provide considerable benefit in discovering valve issues, and can lengthen the time between full valve tests. Finally, the sequences should be designed such that the correct actions can always be executed, i.e. the process may not be in a state where it cannot transition properly.

### **Secure Parameters vs. Non-secure Parameters**

Many of the systems available have a capability for safety communication as well as a normal control network or serial/OPC link. Within the safety network, the data being passed is considered to be secure; there is a higher level of reliability, and a higher level of diagnostics. Quite often there are restrictions places on these safety networks; standard switches and routers are rarely components of these networks. Usually devices are restricted to media converters.

Within the control network or serial/OPC links, there is a lower level of reliability (even though they may be highly available). The data being passed is considered to be non-secure.

It is important to understand that any data that causes a trip must be a secure parameter that is passed on the safety network. In the case of a gasifier there are some scenarios during startup that are hazards as well, so the data involved in this configuration should also be secure.

For all the remaining data involved in either startup or diagnostics, it is adequate to use either the secure safety network or the non-secure control network or serial/OPC link. There is one thing to consider if using non-secure data, and that is the speed of the control network or serial/OPC link. If it is too slow to respond in the desired time, the faster safety network should be used.

### **Partial Stroke Testing and Full Stroke Testing**

In earlier sections we have already discussed using DVC's with partial stroke testing capability. The benefits of partial stroke testing are well known, and nothing further will be said except that for a gasifier, partial stroke testing is used on many valves to ensure that valves are not stuck when needed. This is a reliability requirement.

In addition to partial stroke testing, full stroke testing is used to ensure the valves can *fully close* (or *open*) when needed, so that a startup sequence can be completed successfully. Full stroke tests when the process is cold and at low pressure are not sufficient. Therefore the valves are full stroke tested when the process is warm and at higher pressure, *just prior* to situations in which they are needed. Doing this does add some complexity to the startup sequence, but in this case it is worth it. Full stroke testing benefits reliability, but is used to satisfy the availability requirement. It ensures that the valves will not prevent a startup (availability), and that they will function correctly during a shutdown (reliability).

### **Use of HART data**

HART devices provide additional capability, and they definitely have their place in a SIS. HART protocol is not approved for use in a safety critical application, so it is important to restrict the use of HART protocol to setup, calibration, and diagnostics. The HART diagnostics cannot be used in the reliability calculations, nor can action be initiated by HART variables for a safety trip. The trip is still initiated by the 4-20 mA signals.

With HART information and HART device alerts, the operator can react quickly to issues. In addition, when HART information is analyzed properly, it allows the operator to be proactive and take preventative maintenance when needed. This can increase availability significantly.

Although HART information can not be used to satisfy a SIF, an operating company can choose to trip based on HART information. This has nothing to do with satisfying a SIF, and is what one might call a "common sense" application. These cases are usually rare, since doing this does not benefit reliability, and will lower the availability.

## Implementation Framework

### DeltaV / DeltaV SIS

#### **DeltaV BPCS / DeltaV SIS Architecture**

Because of the way the DeltaV BCS and DeltaV SIS were designed they have some advantages over some of the other systems.

The DeltaV architecture is unique in that the BPCS and SIS share a common platform but are separate systems. The SIS is a certified safety system to SIL 3, is completely integrated with the BPCS, is easy to use, and has a flexible architecture. Because the two systems are integrated but separate, there is no real concern with common cause failures. For availability reasons, both the BPCS controllers and the SIS logic solvers can be redundant. Since the BPCS acts only as the communication interface to the HMI, it is separate from the SIS and cannot interfere with the operation of the SIS. Even if the BPCS has failed, the SIS logic solvers execute logic completely independent from the BPCS, ensuring continued safe operation or shutdown.



Figure 4: Typical DeltaV / DeltaV SIS System

## Centralized Versus Distributed

The DeltaV architecture supports a distributed I/O and controller configuration. Both the DeltaV BPCS and the DeltaV SIS can be installed in remotely located panels, which in this case resulted in significant wiring savings. The system can meet demanding temperature specifications of  $-40^{\circ}\text{C}$  to  $+70^{\circ}\text{C}$ , be installed in hazardous locations, of Class I, Div 2 (Zone 2), and meet the airborne contaminant requirements of ISA-S71.04-1985 Airborne Contaminants, Class G3.

## I/O Count

A fully redundant DeltaV SIS node can accommodate 256 SIS I/O. This is sufficient for a single gasification train. Each logic solver can have up to 8 secure parameters and can reference up to 24 non-secure parameters. There are enough secure and non-secure parameters to handle the trips and permissives for complex sequences such as gasification.

## BPCS/SIS Interactions

With gasification being the complex process that it is, there are numerous interactions between the SIS and the BPCS. The SIS can examine all parameters and variables in the BPCS. For example, the SIS can determine what the current mode of a PID loop is, or it can see the value of a pressure transmitter that is wired to the BPCS. The opposite is also true in that the BPCS can examine, in a non-interfering way, all parameters and variables in the SIS. The BPCS can examine certain conditions and change the mode and/or setpoint of a PID controller, or it may also change the ramp rates of setpoints. The BPCS has no ability to 'write' to the SIS, as the SIS only 'reads' from the BPCS. Configuration of communications between the two systems is done using a browse window. No mapping or special configuration is required.

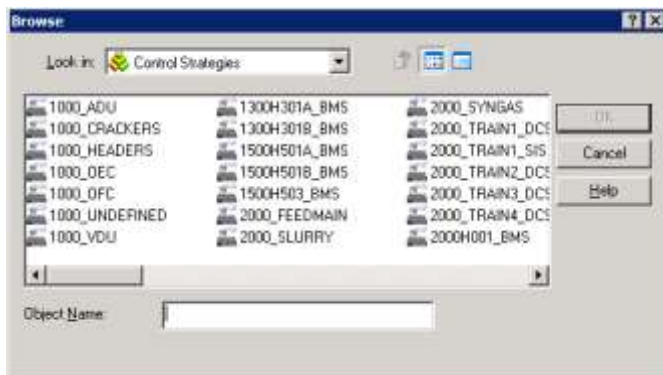


Figure 5: Browse Window

The communication time between the systems is approximately 1 – 3 seconds. This time is the same for both BPCS to SIS communications and SIS to BPCS communications.

## **DeltaV SIS Additional Functionality**

DeltaV SIS also has the additional capability to connect directly to HART I/O without the need for special hardware. The HART data should not be used for safety critical functions, but it can be used for diagnostics and additional process data.

The DeltaV SIS also has built in function blocks for voting as well as for DVC's, with partial stroke testing capability.

## **State Transition Diagrams**

### **STD – Introduction**

A state machine is not something new or recently invented. A state machine is a simple 'pictorial' way of describing how a sequence transitions from one state to the next state. The diagram does not show the details of each state and transition, but gives an overview as to how the sequence will work. In detail, each transition and each state must be described.

State machines have rarely been used in the process industry in the past. Vertical process flow diagrams are by far more common. However, as seen earlier, the state machine, or State Transition Diagram (STD), is a very natural way of looking at a sequenced process.

The figure below is a high level STD for a generic process. The arrows/lines represent the transitions and the circles represent states. The green coloured states represent the states that the process is in most often. The circular nature of a STD represents the true flow of the process through startup, normal operation, shutdown, and maintenance.

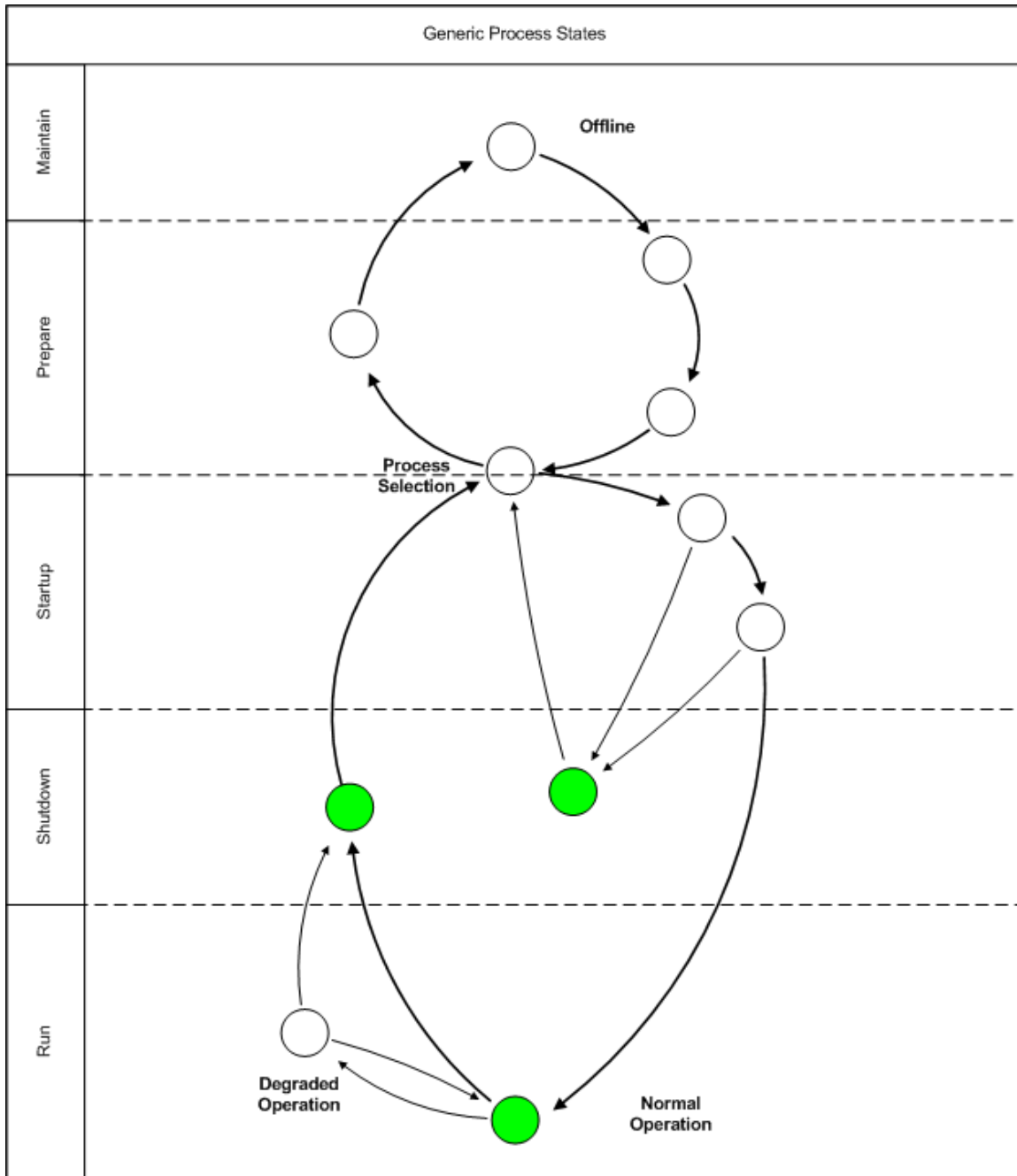


Figure 6: Generic Process Revisited

Every process will not necessarily have all of these states, but these states do cover almost every process. In the most basic terms every sequenced process will have startup, shutdown, and run. A very simple process, or a process one level lower in detail, would probably look more circular in nature. The convention followed here is that the normal path is the path clockwise around the outer edge of the circle.

Although the actual state transition diagrams of a gasification process are proprietary in nature, the figure below shows a fabricated example of a state transition diagram:

**STATE TRANSITION DIAGRAM – EXAMPLE**

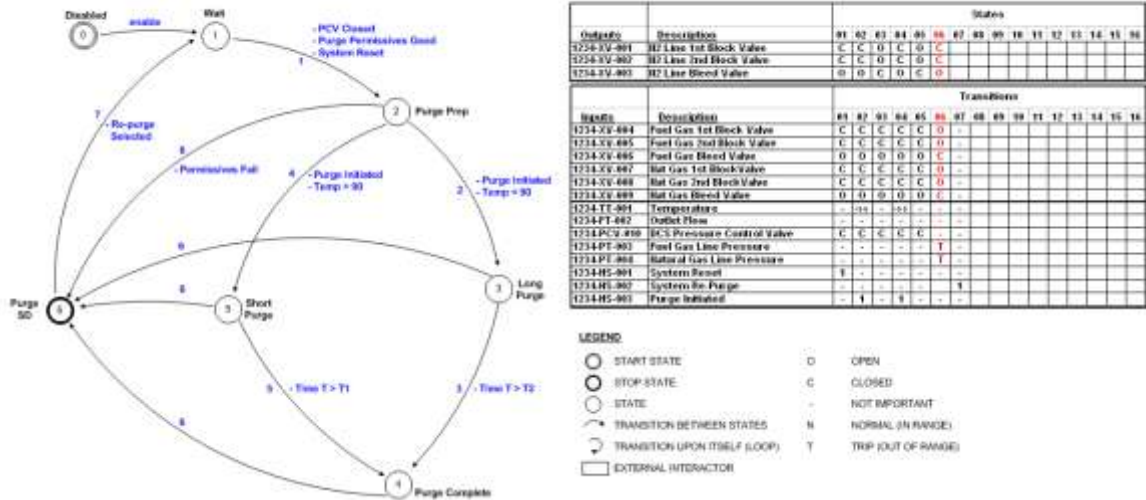


Figure 7: STD Example for a Purge Process on a Burner

**STD - Design Methodology**

For this project the state transition diagram methodology was used for both the written safeguarding narrative as well as in the configuration. This methodology defines every state of the process, including what actions occur in that state (i.e. valve and pump commands) and what permissives are required to get into that state (i.e. valve positions and process measurements). State transition diagrams lend themselves to clearly defining the functional requirements, as well as making it easier for all parties involved to understand and reach consensus on functionality.

**STD – Advantages**

The advantages of using STD’s are that they are easy to change. Adding a state and adding a transition is a simple task. Terminal states (states in which there is no path out) are also easier to see and it is easy to make repairs to these terminal states.

STD’s are very similar to sequential function charts (SFC’s). SFC’s are best used in a very linear top to bottom process. The advantages STD’s have over SFC’s are:

- Easier to see more on one diagram
- Easier to see the “big picture”
- Easier to notice mistakes in transitions
- Easier to find missed transitions
- Easier to lay out nicely

**STD - Built in Function Block**

For DeltaV SIS there are some even larger advantages to using STD's. DeltaV has a built in STD function block. With this function block intuitive descriptions to states and transitions can be added. These descriptions can be used to display the current state of the STD on the HMI. The configuration of the STD block is matrix driven, which allows the user to easily add/remove transitions from one state to another. The STD function can have up to 16 states and 16 transitions. If more states or transitions are required then function blocks can be nested as needed. The ability to nest function blocks allows process engineers and configuration specialists to break a large sequenced process into smaller, more manageable, logical components. It also allows the logic to be distributed amongst several logic solvers, such that the high processing requirement is more manageable. This also makes the configuration easier to build and troubleshoot later on.

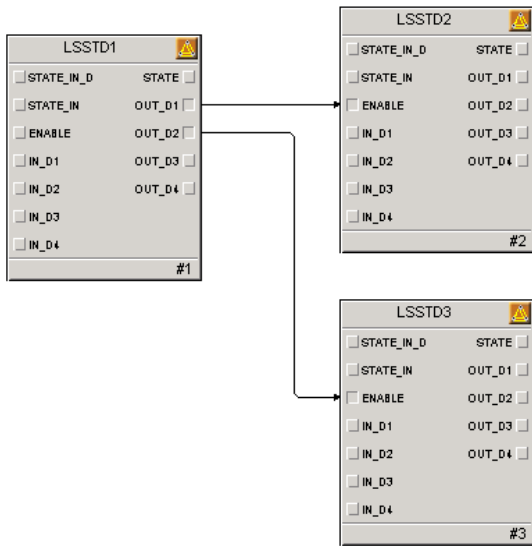


Figure 8: Simple Nesting Example

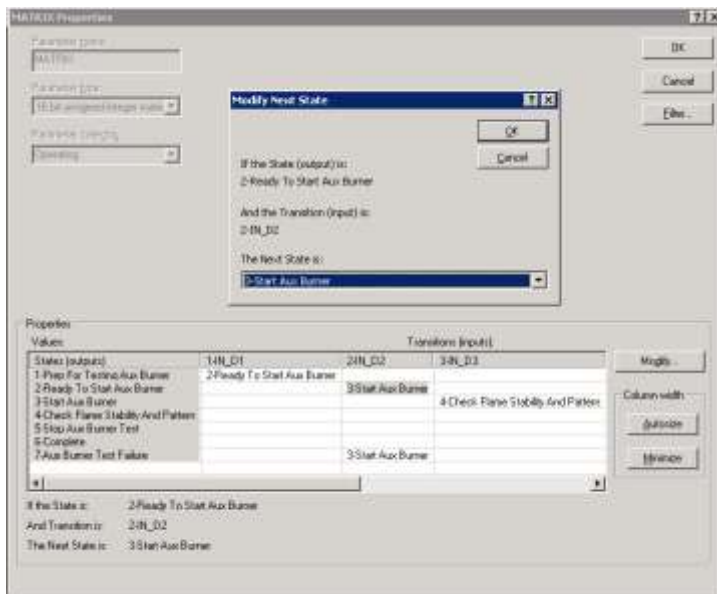


Figure 9: Matrix Configuration of an STD

## Graphics

### Graphics from State Transition Diagrams

For SIS it is very important to have useful, unambiguous, and easy to use graphics. For a sequenced startup it is probably easiest to see the sequence in terms of the state transition diagram that was used for the safeguarding narrative and configuration. Not all of the detailed configuration needs to be shown. The actions within a state are not shown, but the transition conditions are shown. The user may click on a transition line and a window will appear to showing the transition conditions.

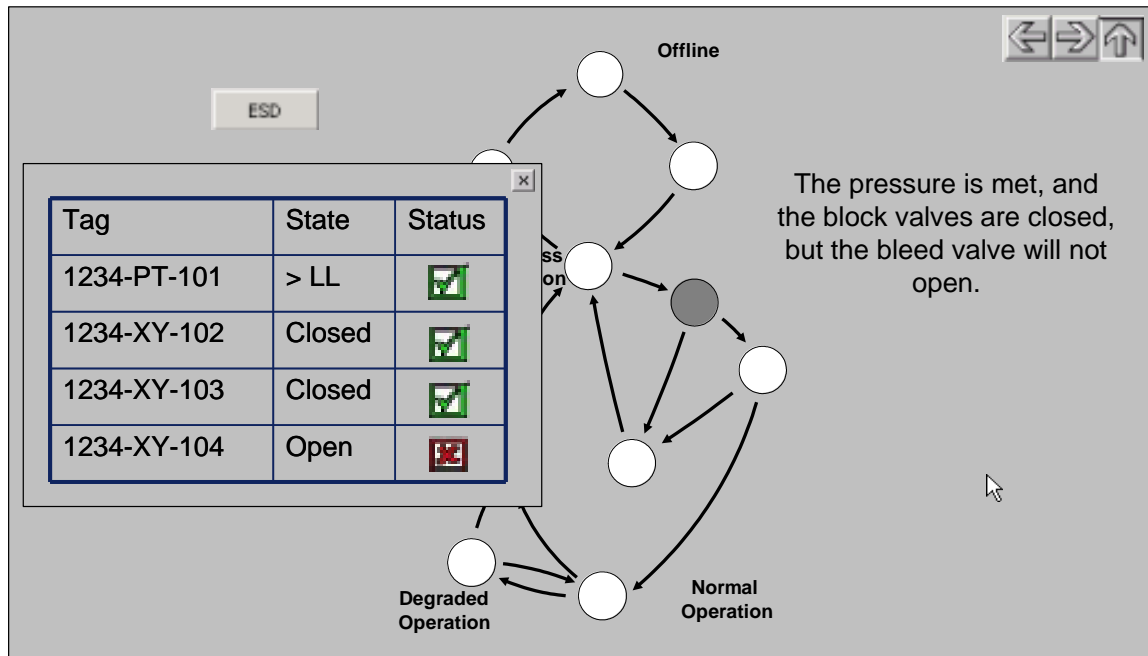


Figure 10: Simple Example showing a Transition Popup

### Quad-Head Monitor Graphics

While the STD graphics are clear, they don't provide all of the information an operator needs for normal process operation of a plant. The plant process flow, process variables, valve positions, etc are not shown on the STD graphic. The STD graphics need to fit within the regular process graphic philosophy, i.e. a multi level graphic system. A quad screen display is very useful for this type of activity. The display structure can remain unchanged, with the STD being displayed on the fourth monitor during startups and troubleshooting (the fourth monitor would normally be used for an alarm screen).

## Conclusions

This exercise has allowed the authors to develop an effective process for evaluating a complex SIS/BPCS application, in a way that lends itself readily to documentation as well as discussion. Using DeltaV BPCS and DeltaV SIS, this translates easily into configuration. This methodology can be used for any process system application.

Several technical issues must be resolved before work can proceed. It is important to have skilled people examine these issues carefully, because they have a large impact on implementation. Once the technical issues have been addressed, implementation can proceed. DeltaV BPCS and DeltaV SIS have some particular advantages that make them an excellent choice. With the right people involved at the right time, and using state transition diagrams in the functional requirements, in the configuration, and for the graphics, efficiency is high which results in cost savings in the long run.

## References

Arnold, J., Bronicki, Y., Rettger, P., Hennekes, B., Hooper, M. de Graff, J., "Gasification in the Canadian Oil Sands: The Long Lake Integrated Upgrading Project", Gasification Technology Conference (GTC) Proceedings. Washington D.C.: GTC 2004

Higman, C., van der Burgt, M., "Gasification", Elsevier 2003

Arnold, J., Rettger, P., Hooper, M., Bronicki, Y., Hennekes, B., de Graaf, J., "Integrated Oil Development Using OrCrude™ Upgrading and Shell Gasification Process", Gasification Technology Conference (GTC). San Francisco: GTC 2002

Kuchle, D., Errington, J., Cushon, G., Bullemer, P., "Human Factors and Operator Interface Design", Parts 1 and 2, Emerson Global User Exchange. Orlando FL 2005.

Center for Chemical Process Safety/AIChE, "Guidelines for Chemical Process Quantitative Risk Analysis (2nd Edition)", 2000.