White Paper
September 2020

State Based Control and the Value Delivered from the Initial Design Through the Operating Life of the Facility

EMERSON™

Table of Contents

Abstract 3
Introduction 3
Knowledge Capture and Transfer 3
Level of Automation 4
State Based Control Adds Value in Early Front End Loading 5
Instrumentation Needs to be Justified 5
State Based Enablement 6
Unit Communication 7
Degradation Scenarios 8
Coordinated Safety Response 10
Standard Reusable Architecture 10
Impact on Unplanned Events 11
Conclusion 12
References 12

Abstract

This paper examines the attributes of automation through state based control and the value delivered to manufacturing from the initial design through the operating life of the facility. It examines both the benefits of improving a non-state based control facility to state based control, as well as the front-end loading of green field project with state based control incorporating instrument and alarm justification into the design process for improved performance and reduced cost. Through knowledge capture and transfer into the control system, this paper demonstrates how state based control will give you, essentially, the best operator on the board performance all of the time. The paper also examines how state based control enhances a traditional single loop safety system with a coordinated safety response. The coordinated safety response manages all outputs of a given unit to a safe state. Communication to other units allows them to remain at their highest state of readiness to return to normal operation reducing process interruption.

Introduction

It should be noted that this paper discusses the value that automation with state based control can add to a facility from initial design through the operating life of the facility. This is in no way meant to imply that state based control is the only way to achieve these objectives. As will be seen, the work process for state based control gives an organized way of adding value in the design and commissioning phases. State based control also provides a solid framework in which to hang the automation and gives a convenient way to communicate between units. That is to say that the same level of automation can probably be achieved with or without state based control, but the framework provided by “states” makes is much easier to accomplish, maintain and improve. As will be seen, it also improves the operability of the control.

There are two types of state based control:

- **Inferred State** – Using process measurements to infer what state the process is in.
- **Driven State** – Using the DCS to drive the outputs to put the process in the desired state.

Knowledge Capture and Transfer

Throughout the life cycle of the facility, knowledge capture and transfer are crucial to successful and safe operation. This process should begin in the early front-end loading (FEL) stages. Sometimes, plants are not started up, commissioned, or operated exactly the way they were designed to be. The involvement of control engineers, process engineers and equipment subject matter experts can capture, during the initial FEL, how the equipment is designed to be operated. This has a tremendous impact on safety and loss prevention, especially when bringing in new equipment or even a new technology that operations personnel are not familiar with. The automation should help operations in a challenging situation rather than confuse the issues at hand with alarm showers. Unproven equipment, operators new to running it and alarm showers are a very bad combination. When equipment is started up according to automated procedures, with no shortcuts, the dynamic alarm management is going to work better and last longer with fewer unplanned events (see the section on the effect of unplanned events). This is a great time to capture the knowledge of the design team and transfer it into the automation where it is always available for use and continuous improvement throughout the lifetime of the facility.

As experience is gained in the plant through the years of operation, learning is going to occur. Sometimes this is learned the hard way - through incidents or near misses. Of course, the knowledge can be captured in procedures, but they can also be captured in automation and automated procedures. This builds the knowledge transfer into the DCS system. Through the operating life of the facility, the automation can become smarter and more robust.

Loss of process knowledge through attrition is often an issue for those facilities that do not have a high level of automation or state based control. A large percentage of the work force is nearing retirement age. Within the next five years, about 20% of the workforce could retire. In a 2012 report, the Social Security Administration estimated 10,000 will retire per day. The younger workforce is going to be smaller and more mobile. Younger workers consider strategic job-hopping normal.

According to the Bureau of Labor Statistics, the average worker stays at each job for 4.4 years. Most millennials expect that they will change jobs every three years or less. For large continuous plants that may not be long enough to even see one turnaround. John Grubbs, author of “Surviving the Talent Exodus”, describes them as the nomadic generation. He points out that only companies that can accelerate the time it takes to make a young worker competent will benefit. They need to become competent quickly enough to be productive until they move on to another opportunity. Knowledge capture and transfer into the automation of the facility can have a huge impact. This knowledge transfer has to happen before the experienced personnel retire.

All of the above knowledge capture can be leveraged to new green field projects with similar process technology through Standard Reusable Architecture. This increases the return on investment in the automation.

Level of Automation

The level of automation needs to be determined early on in the front-end loading. There are a number of considerations in determining what to automate and what level of automation to shoot for.

Part of this will come from the alarm justification process. There are ISA 18.2 metrics regarding operator response. You should keep this in mind when considering the span of control of the operator and the required level of automation. In the determination of Causes, Consequences and Actions, if the required response time from an operator is not realistic, consider automating the response or accepting the consequences that have been identified.

Veronica Lindström and Mats Winroth list some considerations (ref 2):

1. Increase labor productivity
2. Reduce labor cost
3. Mitigate the effects of labor shortages
4. Reduce or eliminate routine manual or clerical tasks
5. Improve worker safety
6. Improve product quality
7. Reduce manufacturing lead time
8. Accomplish processes that cannot be done manually
9. Avoid the high cost of not automating

Consider that operator errors result in the highest average dollar loss per major incident at over $80 million (J. H. Marsh & McLennan, 2010). Also, according to the ACR Advisory Group, operator error accounts for 42% of the unscheduled plant shutdowns with equipment failures and process upsets rounding out the list (O’Brien, 2010).

Historically, trust has been an issue with the level of automation (ref 3) and always will be. In the past, it was more “what do we trust automation to do”, and that is moving toward “what do we trust not being automated” more and more. Certainly, we would want to automate safety shutdown logic with people less and less willing to take credits for operator actions. It is probably not “a matter of time” before we have self-driving cars as much as we will get to the point where we look back and think “it was crazy and dangerous back when we use to drive our own cars around”.

It cannot be overstated - simulation for check out and training is crucial to properly working software working properly and operators’ confidence in automation. With that trust, operators move from manipulating each small part of the process to managing the process with their heads up and getting the big picture. (ref 1,3).

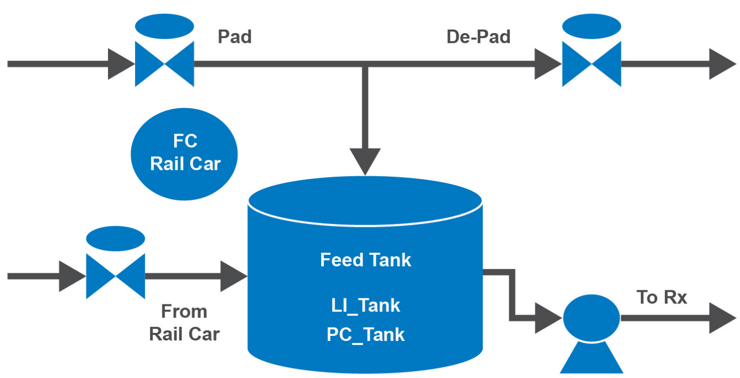
State Based Control Adds Value in Early Front End Loading

Instrumentation is expensive. It has to be purchased, installed, maintained, added to the graphics and configured in the DCS. An instrument is likely to end up with more alarms on it than are needed when its configured in the DCS. This could be because it is easier to add alarms to the instrument than it is to figure out if they are required or not, or just because somebody along the way thinks it should be alarmed. This is the point where alarm rationalization needs to take place. The alarms that are needed should be a factor in determining the instrumentation list. Here are the instruments, now we need to put alarms on them is not the way to go.

Instrumentation Needs to be Justified

If the instrumentation is not deliberately justified for use early in the front-end loading, it causes problems. You may end up with instruments that are not needed, causing unnecessary expense and cost of ownership. Worse yet, instruments that should be there and are not, lead to operability issues. Adding these instruments later on in the project adds much more expense and rework into the project. Before the end of FEL-2, you should have a good list of the instruments that are needed to take forward to the cost estimate. If justified for use, there should be minimal creep through the process.

Given the total cost to install and the cost of ownership, start from the Process Flow Sheets with no instrument. Then add instruments only as the use for the instrument is justified for the appropriate level of automation and alarming. Consider instruments needed for automated startup / shutdown, control, alarms, safety instrumented system, environmental, troubleshooting, redundancy for reliability, and accounting. Then move on to the P&IDs and minimize reworking them.



IO List	Justification
LI_Tank	Safety/Cntl
PC_Tank	Safety/Cntl
CV_DePad	Cntl
CV_Pad	Cntl
FC_Rail_Car	Cntl/Acct
CV_Rail_Car	Cntl

State	PVH_LI_Tank	PVH_PC_Tank	PC_Tank	FC_Rail_Car	PVL_LI_Tank
Maintenance	Emergency	High	DePad		
Manual Line Up	Emergency	High	DePad		
Fill	Emergency	High	Pad / DePad	On / Off Level	Low
Run	Emergency	High	Pad / DePad		High
Run and Fill	Emergency	High	Pad / DePad	On / Off Level	High

Figure 1: Justify the Instrumentation for Use through Each State

Figure 1 is a simple example showing instrumentation justified for use in each process state.

For example, working through bringing the process up in the maintenance state, a high level and high pressure alarm would be needed. Needing a level and pressure alarm justifies the need for the level and pressure instruments. Working through to the fill state, a control valve to fill and a flow transmitter would be required. The flow transmitter would also be used for accounting purposes. Working through starting the unit up in each case instruments are added as justified creating the instrument list and the control narrative. With this process, instruments are not added that are not needed, and instruments that are needed are not missed causing either poor performance or increased cost and rework.

State Based Enablement

An "enable" is fundamentally a decision. It is like a switch to turn something on or off. An enable can let a controller mode be able to operate, or let an alarm ring if the conditions come true. It might also indicate that flow is needed to a control module that manipulates the outputs. In state based control, alarms are pretty strongly based on the process state. For instance, a low level alarm would not be enabled in a process state where the level should be low, like down for maintenance, but enable in the running state. The high level alarm however would probably always be enabled.

Please note that in the discussion below for logic that ∑ will represent a Boolean summation with "Or" logic and π will represent a Boolean product with "And" logic applied through the brackets. So:

∑(A, B, C) = A Or B Or C

π(A, B, C) = A And B And C

For example, a distillation tower may have a number of states in which the steam valve should be open. A first pass at the steam valve logic with respect to states might be:

BV_Steam = State_Heat_Up Or State_Total_Reflux Or State_Recycle Or State_Run

That may not be sufficient in that other state dependent conditions might need to be applied in some but not all of the states.

For example, if the operator should verify the manual line up of the steam system before the steam valve is allowed to operate in the heat up state.

BV_Steam = (State_Heat_Up And Line_Up_ Confirmation) Or State_Total_Reflux Or State_ Recycle Or State_Run

There may be an interlock that applies to all of the states. So the equipment is not operated unless the interlock is false.

For example, don't open the steam valve if there is a high level or temperature no matter what state you are in.

Steam_Valve_Interlock = PVH_Tower_Level or PVH_Tower_Temperature

BV_Steam = [(State_Heat_Up And Line_Up_ Confirmation)
Or State_Total_Reflux Or State_Recycle Or State_ Run]
And Not Steam_Valve_Interlock

Note that the interlock is easily maintained by adding or removing conditions. For instance, adding that there is not a high delta P in the tower. The framework is there.

There may also be instances where a permit is required, which would be a condition that must be true regardless of state to operate the valve.

For example, the cooling system is seen to be in operation because a fan is on.

Steam_Valve_Permit = Fan_Running

BV_Steam = [(State_Heat_Up And Line_Up_ Confirmation)
Or State_Total_Reflux Or State_Recycle Or State_ Run]
And Steam_Valve_Permit
And Not Steam_Valve_Interlock

Why an interlock and a permit? Since the Interlock and Permit act on all of the states, this could be accomplished with just one variable that acts on all the state instead of two. The reason for two is it makes the logic easier to write, troubleshoot and maintain. For interlocks, it is easier to write the "true" logic for the equipment cannot operate. The logic is typically ∑(Condition_i). For permits, they are typically like a daisy chain of condition that must come true in order to indicate that it is ok to operate, π(Condition_i). Both of the lists are easily modified as need be.

All of the above combined gives a basic Unified State Based Control Enablement Theorem:

Permit = π(Condition_To_Allow_Operation_In_Any_ State_i)
Interlock = ∑(Condition_To_Interlock_Operation_In_ Any_State_i).
Enable = [∑(State_i) And π(State_Dependent_ Conditions _i)]
And Permit
And Not Interlock

Where it is understood that some states may not have a special condition for that state and a Permit or Interlock may or may not be needed.

The above equations can be used in state based control as an organized robust means of enabling many things based on the state.

The above form of the enablement equation can be used to open a steam valve as mentioned above or enable alarms or controller modes. It can also be used to trigger sequences in control or equipment modules. For instance – it can calculate when a fuel gas flow is required and send the signal to a double block and bleed module. Upon receiving the signal for flow or stopping flow it will sequence the bleed, upstream and downstream valves. Likewise, a pump with a suction, motor and discharge valve module could receive an instruction that flow is required or not required and in the same way sequence the suction, motor, and discharge outputs to achieve flow or stop flow.

Unit Communication

Within a process, cell units provide services to other units and require services from other units to make the product. For instance, a raw material feed tank may provide feed to a reactor as a service, but requires the thermal oxidizer to treat vents from the tank's pad/de-pad system. This becomes very important in properly starting up the process as well as normal shutdowns, emergency shutdowns and degradations where the process is not shutdown, but not 100% where you would want it to be.

In a similar fashion to the state based enablement, Boolean logic can be constructed based on the states to signal when a unit needs, is requesting, or can provide a service to the process. This may be all that is needed or could go to something like the ISA 88 States.

For instance, a Boolean can be created in the Thermal Oxidizer unit communicating that it can provide vent treatment. Within each unit that requires the thermal oxidizer in the state transition logic, the Thermal_Oxidizer_Can_Provide_Vent_ Treatment flag is required to move to a state where it will create vents that need to be treated. Each unit that requires vent treatment can construct a similar Boolean based on the states that it needs vent treatment. For instance, Feed_Tank_Needs_ Vent_Treatment. Within the thermal oxidizer, the transition logic will check that no units need vent treatment before it transitions out of a state where it can provide it, unless it is required for a safety trip. The safety trip scenario will be discussed in the degradation scenario section.

There are several advantages to the Booleans based on state. One is that individual developers may not know that much about other units that they are not working on. For instance, if the guy doing the feed tank doesn't know that much about the thermal oxidizer, he knows that he needs it and that by convention the developer will create a flag when it can treat vents. Likewise, the developer of the thermal oxidizer knows that all users by convention will create a flag that they need vent treatment.

Another advantage to the communication Booleans is that they enforce a normal proper start up and shutdown of the process. The thermal oxidizer has to come up first before the units that require vent treatment can come up, and they must go down first before the thermal oxidizer can come down. This will eliminate being able to come up without environmental devices that are required by the permit to operate the facility. This prevents environmental issues, fines or loss of license to operate.

They provide an easy way to identify and deal with degradation scenarios.

Degradation Scenarios

If things work normally, the units will come up and down as needed based on when they can provide or need services. What happens when a service is needed but cannot be provided, as in the case of a thermal oxidizer trip? For instance, the feed tank would not be allowed to transition to a state where vent treatment was needed without it being available. After it is up and running, what happens when the vent treatment service can no longer be provided? If something is needed but cannot be provided it is a degradation scenario.

The state based control can be structured to keep the process at its highest state of readiness, given the degradation, so that it can return to normal operation as quickly as possible.

So in the case of the above mentioned degradation, depending on the mechanical layout of the plant and what the plant is permitted to do, the solution that causes the least problems can be implemented when the degradation is detected. For instance, if the operating permit allows venting to the atmosphere until the thermal oxidizer can be restarted, the system could vent for a short time. However, if venting is not permitted and a flare header is available, then vent to the flare header.

Since each unit can communicate what it needs and what can be provided, a matrix of degradation scenarios can be created to always keep the plant at the highest state of readiness. As another example, if the reactor that is providing feed to the finishing section trips it can move to a total reflux or recycle state until the reactor comes back online.

As an example, consider a process with a feed tank, a reactor, a distillation tower, and a thermal oxidizer. In order to keep the example brief, just a few services and scenarios are shown (not intended to be comprehensive).

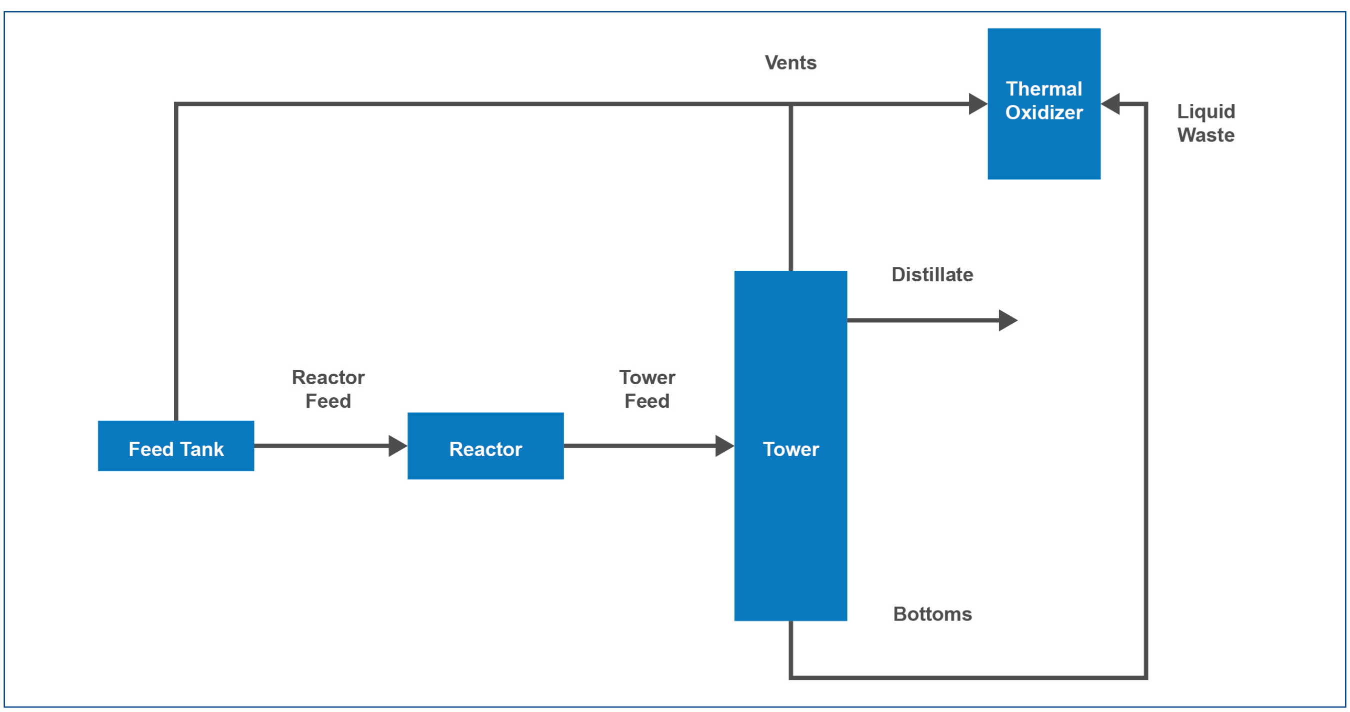


Figure 2

Unit	Service Provided 1	Service Provided 2	Service Provided 3
Feed Tank	Provide Feed to the Reactor		
Reactor	Taking Feed from the Feed Tank	Provide Feed to Tower	
Tower	Taking Feed from the Reactor	Providing Ditillate	Providing Bottoms
Thermal Oxidizer	Vent Treatment	Liquid Waste Treatment	

Table 1. Services Provided

Unit	Service Provided 1	Service Provided 2	Service Provided 3
Feed Tank	Vent Treatment		
Reactor	Feed from the Feed Tank		
Tower	Feed from the Reactor	Vent Treatment	Liquid Waste Treatment
Thermal Oxidizer			

Table 2. Services Used

Since it is known that degradation occurs if we lose something that is being provided, a degradation matrix can be created to give the required actions. Please note that the action does not necessarily have to be automated. It is a better idea to figure out what needs to happen, and then decide which things will be automated.

Unit	Thermal Oxidizer can't Treat Vents	Thermal Oxidizer can't Treat Liquid Waste	Feed Tank can't Provide Reactor Feed	Reactor can't Feed the Tower	Tower can't Take Feed from the Reactor
Feed Tank	Switch Vents to the Flare Header		XXXXX	Stop Feeding the Reactor	Stop Feeding the Reactor
Reactor			Flush with Solvent and Swap to Solvent Recovery	XXXXX	Flush with Solvent and Swap to Solvent Recovery
Tower	Switch Vents to the Flare Header	Switch Tower Bottoms to the Burn Tank (If Burn Tank Level becomes too high, go to Total Reflux)		Go to Total Reflux	XXXXX
Thermal Oxidizer	XXXXX	XXXXX			

Table 3. Degradation Matrix

This exercise is very useful in discovering operability issues early. For instance, with the “Thermal Oxidizer Can’t Treat Liquid Waste” degradation, if there is not a Burn Tank in the process design, the tower would have to go to total reflux and stop production in the plant. The plant production could have been hanging on a flame detector. In general, a detailed study of using automation to bring the plant up can uncover start up issues and avoid the “we have to build it running, because there is no way to start it up” syndrome.

History trending the communication Booleans can be very beneficial for troubleshooting as well since they will indicate when degradation have occurred.

Coordinated Safety Response

A trip from the safety system will in all probability result in a degradation scenario. A piece of equipment that was needed to provide something is gone. With this degradation recognized in the control system, the process can automatically remain at the highest possible state of readiness under the current circumstances.

The safety system without state based control is designed well and tested to achieve the desired probability of failure on demand. The safety instrumented function will protect against the scenario for which it was designed. It will also cause many operability problems that have to be dealt with by the operator manually when it activates. What follows in trying to deal with the trip may inadvertently lead to the next trip / incident.

For instance, if a SIF cuts steam to a reactor to prevent an over pressure situation the reactor is probably not going to over-pressure and rupture. But what else has to happen to deal with the trip? You are probably in a high stress situation, maybe in high stress situation, such as an alarm shower. Do you stop the feeds to the reactor? Do you leave one feed running to prevent polymerization and cut another one off to stop the exotherm? Do you go to full cooling? Do you vent to the flare header? Would doing any of those things cause more problems? In the midst of this, the back end of the plant has just lost feed and it will all have to be dealt with manually while getting the reactor squared away.

It would be a lot better to have the most experienced operator on the board, when he is well rested and having a good day. A less experienced board operator may have never seen this scenario and there is not time to go get the procedures. Even the most experienced board operator may be fatigued or under a lot of stress.

With automation, you not only have the best board operator on all the time, but you also have the cumulative knowledge from the design team along with what has been learned about the plant through start up and commissioning and operation to this point.

Standard Reusable Architecture

To save cost and improve quality whenever possible, embrace the use of a standard reusable architecture. “State based control has been implemented and standardized for some time through ISA S88. It is often associated with batch processes but works equally well for continuous processes. S88 was written to improve efficiency. It provides a standard way to specify equipment and control modules in an architecture that can be re-used. ISA 106 Procedure Automation for Continuous Process Operations is in development.”(ref 1). For more detailed information on the ISA 88 physical model see, ISA 88.

On a very high level, a unit module can be thought of as something on the order of a unit operation, like a reactor for instance. The architecture can be structured such that the unit module is made up of equipment modules. An equipment module might be on the order of a charging system. The charging system may be a grouping of a number of different things like valves, pumps, screw conveyers, etc. that work together to provide the reactor charge. The final actuators of the equipment module may be in control modules that actually interface with the IO. So, the equipment module may contain a number of control modules. The control module implements the basic control.

Once investments are made in the development of Control, Equipment and Unit Modules, they can be reused as applicable. For instance, a reactor to make a product may need to feed in a particular reactant to a given amount for the batch size, at a rate, with certain constraints. To make the product, these things are not going to change. There may be a facility in a large integrated site that has a header that can provide the reactant. In another site, it may be stored in a tank. In another site, it might be put on totes and weighed in.

With proper consideration to architecture, a unit module can be built for the reactor that is isolated from the variability in the instrumentation by control modules, essentially driving as much variability as possible into the control modules. So, the unit reactor module can be used for any application of the reactor. Control and equipment modules can be built to deliver the flow of reactant according to the parameters specified from the reactor unit module. There may be reuse of the control and equipment modules as well. For instance, the tote may have application in other places.

In terms of skill set, the reactor is going to require a great deal of process knowledge and process control expertise. Building control and equipment modules to deliver an amount of flow at a given rate will probably take a little less expertise. The instantiation of previously created unit, equipment and control modules will probably take even less expertise. So in effect, this leverages the process and process control knowledge.

Impact on Unplanned Events

Unplanned events in a manufacturing facility are expensive and dangerous. “Some analysis has been done linking unplanned events to alarm rates and the level of automation of a facility, with the facilities divided into four quadrants.” (ref 1)

As you might expect quadrant one with low alarm loading and high automation was the least likely to have unplanned events. Quadrant 4 with high alarm loading and low automation was the most likely to be have unplanned event.

With the recent emphasis on alarms, it should be noted that comparing Quadrant 2 with high alarm loading and a high level of automation to Quadrant 3 with low alarm loading and a low level of automation that Quadrant 2 had less unplanned event than quadrant 3.

It can be seen from the slope on the surface of the alarm loading axis that alarms are important, but the surface on the automation axis has twice the slope of the alarm axis in the reduction of unplanned events.

Quadrant 2	Quadrant 4
High Alarms High Automation	High Alarms Low Automation
Quadrant 1	**Quadrant 3**
Low Alarm High Automation	Low Alarms Low Automation

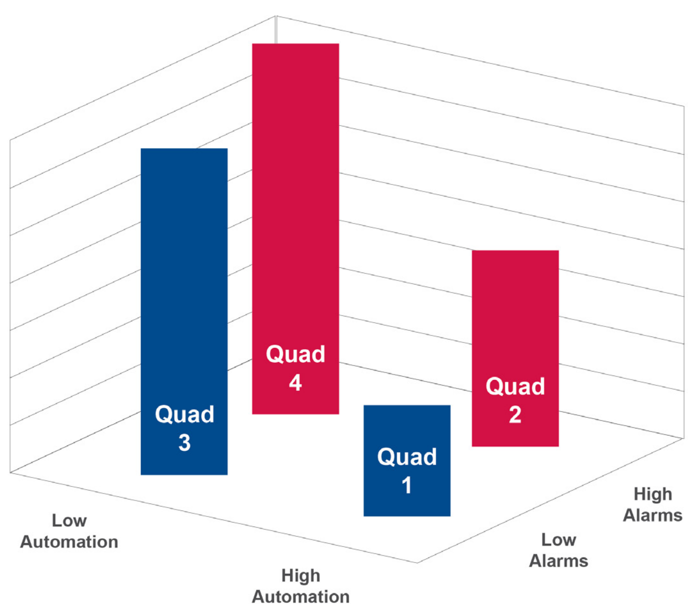


Figure 3: Relative Unplanned Events by Quadrant

This is a very significant opportunity. Alarm management is important, but automation can have twice the impact.

Conclusion

Addressing automation through state based control from the early front-end loading stages can be a systematic way of justifying instruments and dynamic alarm management. It can also reduce cost and improve performance of a facility. State based control gives you the ability to capture and transfer knowledge (from the original design team through start up and commissioning and then ongoing run time) in order to keep equipment operating as it was designed, for safer more reliable and economical operation. The plant can get smarter with time and that knowledge can be embedded in the control system for whoever is on the board regardless of experience level. It is never too late to start. Automation can be added in as a consideration from the beginning of the facility or added in at any time. A reusable architecture will increase the return on investment in automation while improving quality and consistency.

Operators are in a position to manage the process through state changes while having their heads up to see the big picture - avoiding problems and optimizing performance. Managing alarms is important in the reduction of unplanned events. Automation can have an even larger impact on reducing unplanned events than alarm management. Bottom line alarm management and automation are both things that need to be addressed for a safe productive plant.

State based control allows project teams to meet and exceed the rising expectations they are challenged with.

References

[1] 1.0 Change Your Board Operator to a Process Manager with State Based Control (Tom Nolan with Katherine Persac)

[2] 2.0 Aligning manufacturing strategy and levels of automation: A Case Study (Veronica Lindström and Mats Winroth)

[3] http://www.diva-portal.org/smash/get/ diva2:355948/fulltext01.pdf

[4] 3.0 Determining Appropriate Levels of Automation FITS SRM Automation Management Research (Charles L. Robertson)

[5] https://www.faa.gov/training_testing/training/ fits/research/media/Det_App_Lvl_Atm.pdf

[6] http://www.controlglobal.com/articles/2003/181/

[7] https://www.isa.org/isa88/

Contact Us
www.emerson.com/contactus

EMERSON