InTech FOCUS

An *InTech* ebook covering the fundamentals of automation

MAY 2021

Process Control & Safety

IEC 61511 Operation and Maintenance

Closed-Loop AI for Autonomous Processing

Case Study: Petronas Digital Transformation

Automatic SIS Configuration

Introduction

The arrival of new technologies continues to impact the process automation industry. Digitalization and innovation are transforming process control and process safety, and automation professionals are critical to successfully selecting and applying new technologies. Some say the move from automated to autonomous process manufacturing is right around the corner, enabled in part by closed-loop artificial intelligence applications. Others, such as PETRONAS, are already doing what they can to create new strategies and implement new techniques for operational excellence, digitalization, and remote operations across multiple sites.

At the same time, the adoption and periodic revision of IEC 61511 and IEC 61508, the leading standards influencing process safety, have established performance-based criteria for evaluating safety instrumented systems (SISs). This has steadily shaped improvements, shifting from a strictly prescriptive methodology to a more performance-based methodology. Documenting the performance of a plant's SIS ensures it can fulfill its designed requirements, while automatic configuration of an SIS can provide a consistent approach with fewer errors and less rework.

InTech Focus is an electronic periodical from ISA, brought to you in conjunction with Automation.com. This series of electronic magazines focuses on the fundamentals of essential automation components, such as instrumentation, final control elements, HMI/SCADA, and more. View and subscribe to *InTech* magazine and *InTech Focus* at https://isa.org/intech.

Find other ebooks in the series at https://www.automation.com/en-us/resources-list-pages/intech-focus-ebooks.

Renee Bassett, Chief Editor
rbassett@isa.org

Our Sponsors:

exida®

Quartic.ai

ASSURED AUTOMATION®

ISA GLOBAL CYBERSECURITY ALLIANCE™

In This Issue

Upcoming Issues:

September: Electrical Systems & Control Panels

November: SCADA, HMIs, & Mobile Devices

Account Managers:

Chris Nelson
+1 919-990-9265
cnelson@isa.org

Richard Simpson
+1 919-414-7395
rsimpson@isa.org

Gina DiFrancesco
+1 216-509-0592
gina@isa.org

exida, your partner for moving forward

As a global leader in dependable automation, exida has the experience and knowledge to help you move your organization forward. exida provides Lifecycle Services, Enterprise Tools, Assessments, and Certification for our customers **functional safety**, **cybersecurity,** and **alarm management** needs.

Expertise and Insight

Clients rely on exida to help solve their toughest challenges. We meet our customers where they are, from triage to evidence-based decision making, and working with them create the roadmap to move forward. Projects include advisory services, engineering services, and enterprise tool suites.

Advisory Services – understanding what needs to be done and the best way to do it is critical to success. exida supports customers with functional safety assessments, benchmark studies, strategy development, and program management.

Engineering Services – once the plan is set it is time to get it done. exida's safety and cybersecurity engineers help get the work done whether it is a PHA, LOPA, SIL Verification, Proof Test Specification, Alarm Management, or Cybersecurity Risk Assessment and Mitigation.

exSILentia Enterprise Tool Suite – capturing information and knowledge is essential to ensure the gains of a project are sustained. The exSILentia Tool Suite is a total lifecycle solution for your functional safety, cybersecurity, and alarm needs.

www.exida.com

Complying with IEC 61511 Operation and Maintenance Requirements

By Dr. Steve Gandy CFSP, DPE, MBA, DipM;
exida Engineering LLC

It is hard to believe that the IEC 61511 standard has been in existence since 2003, and most companies operating in the process, chemical, and refining industries—or any other hazardous process manufacturer—have adopted its practices. It is also significant that any plants that were built at that time with safety instrumented systems (SISs) will now be halfway through their useful life. This raises the question of how well companies have been recording the performance of their SIS in terms of failures, spurious trips, time to repair/restore, and proof testing results. The new 2016 edition of IEC 61511 emphasizes this need more strongly in terms of preventing systematic issues through procedures and competency. This article highlights how testing and documenting the performance of the SIS is an essential part of ensuring it can fulfill its designed functional safety requirements. This is especially true as the SIS approaches its end of useful life.

Testing and documenting the performance of an SIS is an essential part of ensuring it can fulfill its designed functional safety requirements.

Over the past two decades, automation has constituted one of the dominant factors used by chemical and petrochemical industries in cost reduction efforts. Automation has been characterized by staff layoffs, and the few who remain are not only exposed to prolonged work hours but also are struggling to cope with the increasing work demands. Coupled with the shortage of skilled employees, the condition is even worse when more complex instrumentation and automation systems are introduced.

In the face of such challenges, the introduction of the IEC 61511 standard for the process industries has steadily shaped safety improvements through the safety life cycle (SLC). This is a shift from a strictly prescriptive methodology to a more performance-based methodology. The objective is risk reduction. This article will not define the application of the standard but will examine one important aspect of the SLC: the operations and maintenance (O&M) requirements for the plant SIS.

IEC 61511-1 Clause 16: SIS Operations and Maintenance

The use of the SIS term, contrary to the safety system, is based on the existence of numerous safety systems, but not all are in compliance with IEC 61511. Only safety instrumented functions (SIFs) that are part of safety instrumented systems are required to comply as represented in figure 1.

In IEC 61511-1 Clause 3.2.72, SIS refers to an SIS meant to implement one or more SIFs and is made of any combination of sensor(s), logic solver(s), and final element(s), as illustrated in figure 2. An SIS can include either safety instrumented control functions, safety instrumented protection functions, or both. An SIS also may include software.

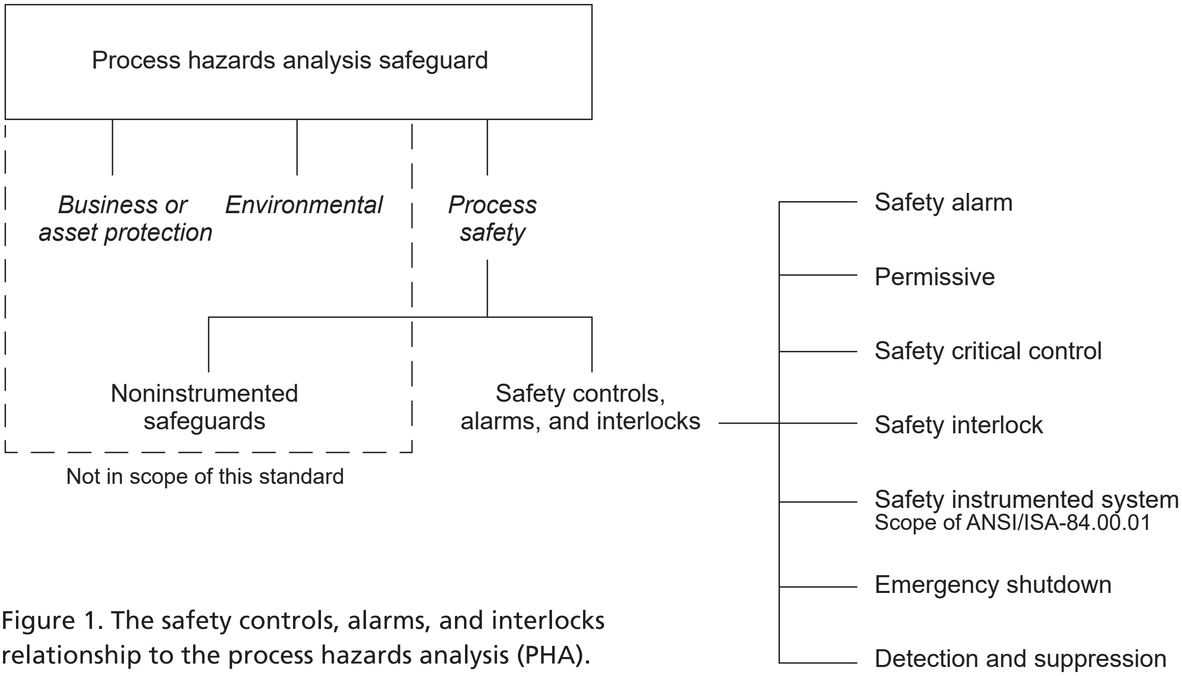


Figure 1. The safety controls, alarms, and interlocks relationship to the process hazards analysis (PHA).

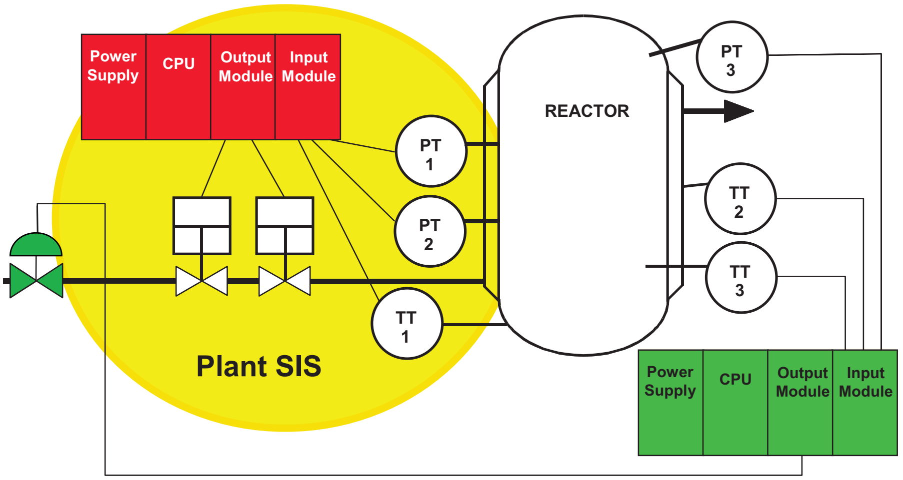


Figure 2. Example of a safety instrumented system block diagram.

To fulfill IEC 61511-1 Clause 16 requirements, an adequate operation and maintenance plan is required by the end user in meeting the required safety integrity level (SIL) of each SIF during operation and maintenance tasks to ensure maintenance of function and integrity of the SIS (figure 3).

The importance of lagging and leading indicators

The IEC 61511 is a "performance-based" standard that requires the owner/operators to undertake "periodic" assessments to identify:

- near misses
- trips—real and spurious
- faults—random and systematic
- process upsets.

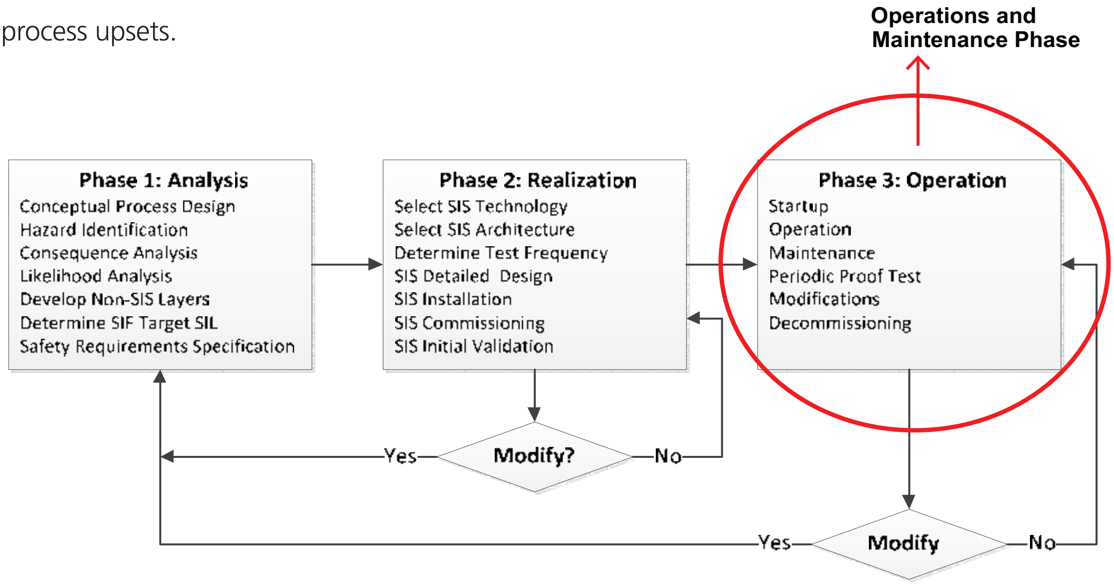


Figure 3. Simplified functional safety life-cycle diagram.

The purpose of lagging data is to assist in preventing future problems, developing training programs, and improving procedures. The purpose of leading indicators also is to help predict future events, which may include overdue inspections and late maintenance challenges.

Through a clear understanding of the leading and lagging indicators, effectiveness and efficiency can be enhanced.

Operations and maintenance plan

The O&M plan is a working document tailored to ensure SIS maintenance meets its designed functional safety and entails:

- routine and abnormal operation activities
- proof testing
- procedures, measures, and techniques ideal for operation and maintenance
- verification of adherence to protocols
- period for undertaking such activities
- identity of the stakeholders.

> “An SIS can include either safety instrumented control functions, safety instrumented protection functions, or both.”

Operation and maintenance procedures

IEC 61511-1 Clause 16.2.2 mandates the creation of O&M procedures with the relevant safety planning and provides:

- routine actions that need to be carried out to maintain the “as designed” functional safety of the SIS such as proof test intervals
- requisite actions and constraints in risk mitigation
- system failure and demand rates–related information
- audits and tests-related information
- the maintenance procedures in case risks occur, including:
  - fault diagnostics and repair procedures
  - revalidation procedures
  - maintenance reporting requirements
  - tracking performance procedures
  - properly calibrated and maintained tools.

These requirements place a heavy burden on the O&M personnel who need to have the requisite skill set to be able to maintain the SIS. In addition, the O&M personnel will be required to follow a written proof test procedure as defined in IEC 61511-1 Clause 16.2.8. The proof tests will need to cover the entire SIS including the sensor(s), the logic solver, and the final element(s) (e.g., shutdown valves and motors). In addition, the proof tests will need to be carried out at intervals that were specified and used to calculate the PFD_{avg} for the SIF. The implication is that personnel training is a key element to ensuring the SIS can be maintained and operated correctly.

What happens in practice?

To adhere to the IEC 61511-1 Clause 16 provision, adequate documentation and tracking system knowledge is vital to follow adequate procedures. It remains to be seen how diligent the personnel are at recording this data, since it depends on the plant's safety culture as reported in the Tesoro incident in 2010, which resulted seven deaths.

How data is recorded

Most basic process control systems (BPCS) need a historian logging trips, alarms, and diagnostic faults for archiving plant data. Normally, this type of data associated with the SIF also is recorded in a historian. Besides, the purpose of proof testing is to reveal undetected faults, and it must be undertaken pursuant to the written procedure. When proof test coverage is included, the frequency and thoroughness of manual proof testing will be assured.

IEC 61511-1 Clause 16.3.3 also demands records storage certifying that proof tests and inspections were completed and includes:

- outline of tests and inspections
- tests and inspection dates
- identity of the individual performing tests and inspections
- unique identifier of the system tested
- results of the tests and inspection.

Technology can help

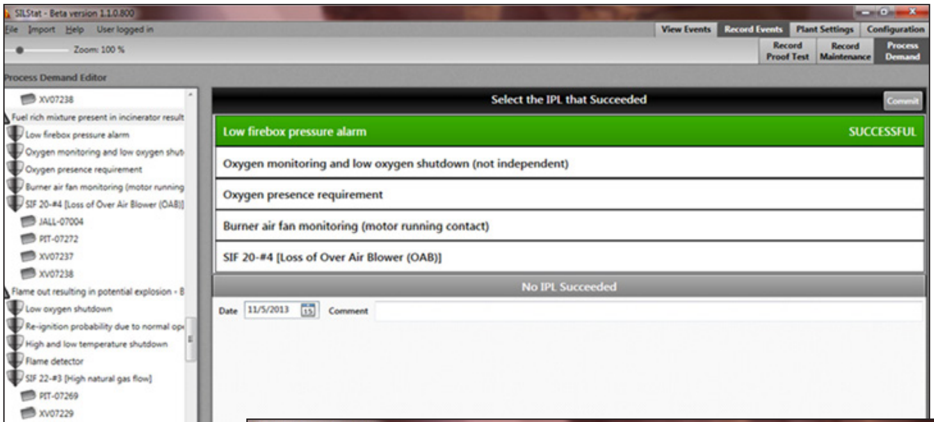
Currently, handheld tablets are widely used in recording data in electronic format. However, having a dedicated tool specifically designed for this purpose remains a challenge. Consequently, O&M personnel rely on Excel spreadsheets to supplement paper-based systems.

O&M personnel would need a tool that can record functional safety-related statistics/performance metrics, as well as life events such as:

- demands—both real and spurious
- inspection and proof test results
- maintenance activities
- failure reporting.

Recording demands such that the user can determine which protection layer failed is another important aspect because the information provided would enable the user to determine the demand frequency of the hazard scenario and initiate a corrective action (figure 4).

The information also could be used to determine the demand frequency of the hazardous event (figure 5).



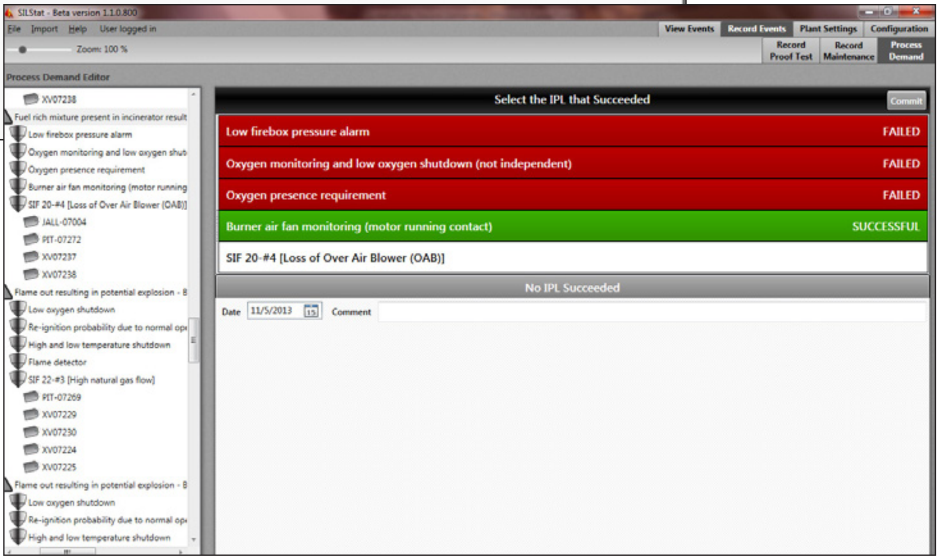
Select the IPL that Succeeded

Low firebox pressure alarm	SUCCESSFUL
Oxygen monitoring and low oxygen shutdown (not independent)	
Oxygen presence requirement	
Burner air fan monitoring (motor running contact)	
SIF 20-#4 [Loss of Over Air Blower (OAB)]	

No IPL Succeeded

Date 11/5/2013 Comment

Figure 4. Example template for recording successful demands on the SIS.



Select the IPL that Succeeded

Low firebox pressure alarm	FAILED
Oxygen monitoring and low oxygen shutdown (not independent)	FAILED
Oxygen presence requirement	FAILED
Burner air fan monitoring (motor running contact)	SUCCESSFUL
SIF 20-#4 [Loss of Over Air Blower (OAB)]	

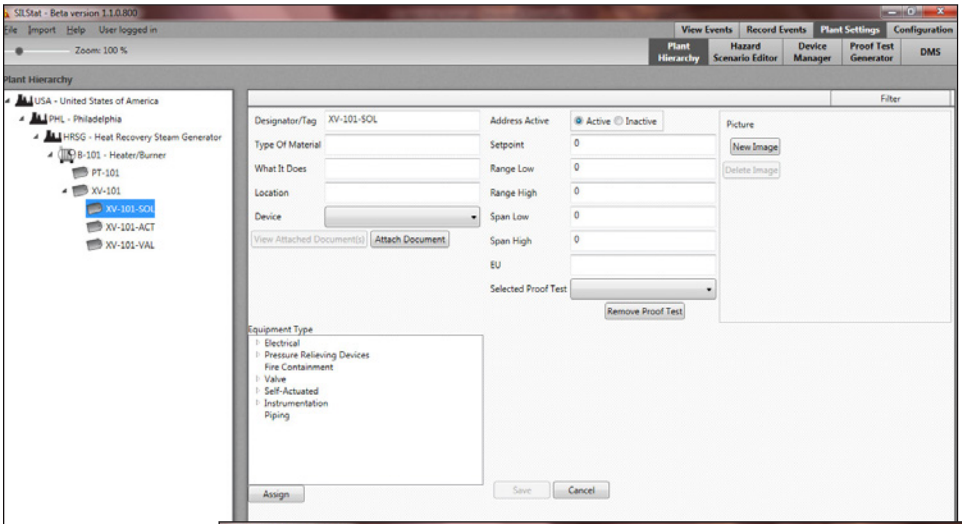
No IPL Succeeded

Date 11/5/2013 Comment

Figure 5. Example template for recording unsuccessful and successful demands on the SIS.

Having a tool that enables the storage of physical devices of the SIS in a database and identifies them by their associated tags and/or descriptions will enable O&M personnel to enhance efficiency in undertaking replacement procedures (figure 7).

Giving the O&M personnel an automatic proof test generator that allows them to specify individual proof test steps with pass/fail criteria would be a significant benefit (figure 8). This would allow the O&M personnel to only record factual data during a proof test.



Plant Hierarchy

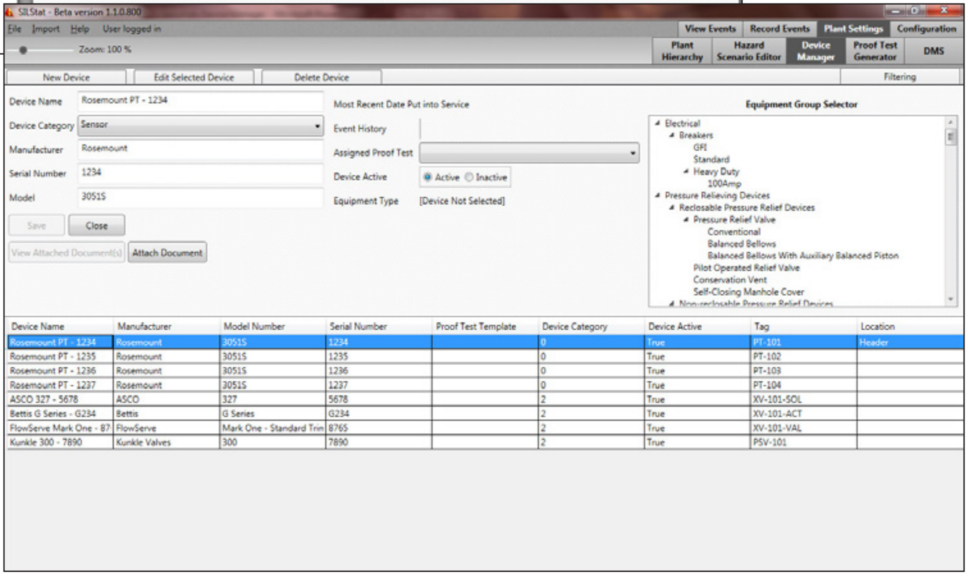
- USA - United States of America
  - PHL - Philadelphia
    - HRSG - Heat Recovery Steam Generator
      - B-101 - Heater/Burner
        - PT-101
        - XV-101
          - XV-101-SOL
          - XV-101-ACT
          - XV-101-VAL

Designator/Tag: XV-101-SOL
Type Of Material:
What It Does:
Location:
Device:
Address Active: ● Active ○ Inactive
Setpoint: 0
Range Low: 0
Range High: 0
Span Low: 0
Span High: 0
EU:
Selected Proof Test:
Picture

Equipment Type

- Electrical
- Pressure Relieving Devices
- Fire Containment
- Valve
- Self-Actuated
- Instrumentation
- Piping

Figure 6. Example template for recording plant hierarchy.



Device Name: Rosemount PT - 1234
Device Category: Sensor
Manufacturer: Rosemount
Serial Number: 1234
Model: 3051S
Most Recent Date Put into Service
Event History
Assigned Proof Test:
Device Active: ● Active ○ Inactive
Equipment Type: [Device Not Selected]

Equipment Group Selector

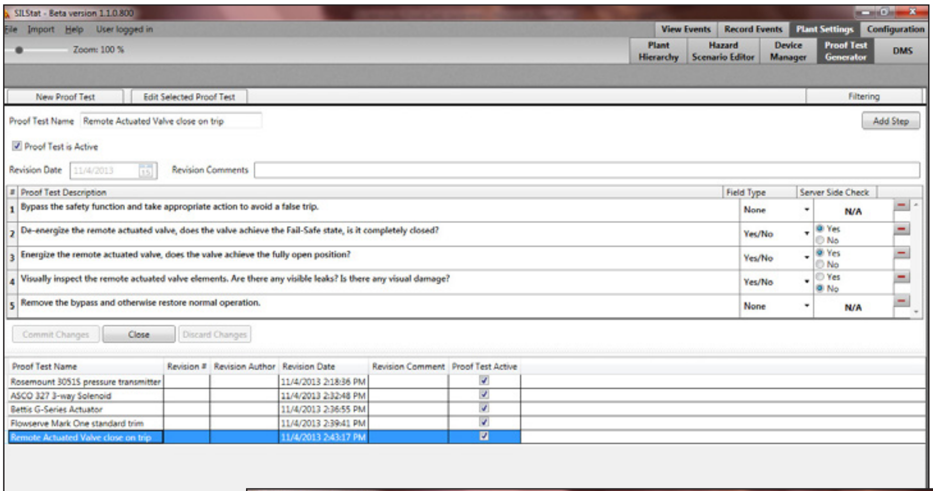
- Electrical
  - Breakers
    - GFI
    - Standard
    - Heavy Duty
      - 100Amp
- Pressure Relieving Devices
  - Reclosable Pressure Relief Devices
    - Pressure Relief Valve
      - Conventional
      - Balanced Bellows
      - Balanced Bellows With Auxiliary Balanced Piston
    - Pilot Operated Relief Valve
    - Conservation Vent
    - Self-Closing Manhole Cover
  - Non-reclosable Pressure Relief Devices

Device Name	Manufacturer	Model Number	Serial Number	Proof Test Template	Device Category	Device Active	Tag	Location
Rosemount PT - 1234	Rosemount	3051S	1234		0	True	PT-101	Header
Rosemount PT - 1235	Rosemount	3051S	1235		0	True	PT-102	
Rosemount PT - 1236	Rosemount	3051S	1236		0	True	PT-103	
Rosemount PT - 1237	Rosemount	3051S	1237		0	True	PT-104	
ASCO 327 - 5678	ASCO	327	5678		2	True	XV-101-SOL	
Bettis G Series - G234	Bettis	G Series	G234		2	True	XV-101-ACT	
FlowServe Mark One - 87	FlowServe	Mark One - Standard Trin	8765		2	True	XV-101-VAL	
Kunkle 300 - 7890	Kunkle Valves	300	7890		2	True	PSV-101	

Figure 7. Example template for recording and managing devices.

Problems found during proof testing need to be repaired pursuant to IEC 61511-1 Clause 16.3.1.4. Although the standard doesn't specify a particular time period, the mean time to restore (MTTR), as used during the SIL determination of the SIF(s) and for the PFD_{avg} calculation, must be followed to restore the SIS to its safe state as soon as possible. Having the ability to identify and rectify deficiencies quickly and effectively is the key (figure 9).

The ability to record these maintenance activities via a handheld or mobile device would simplify the O&M personnel's job.



Proof Test Name: Remote Actuated Valve close on trip

☑ Proof Test is Active

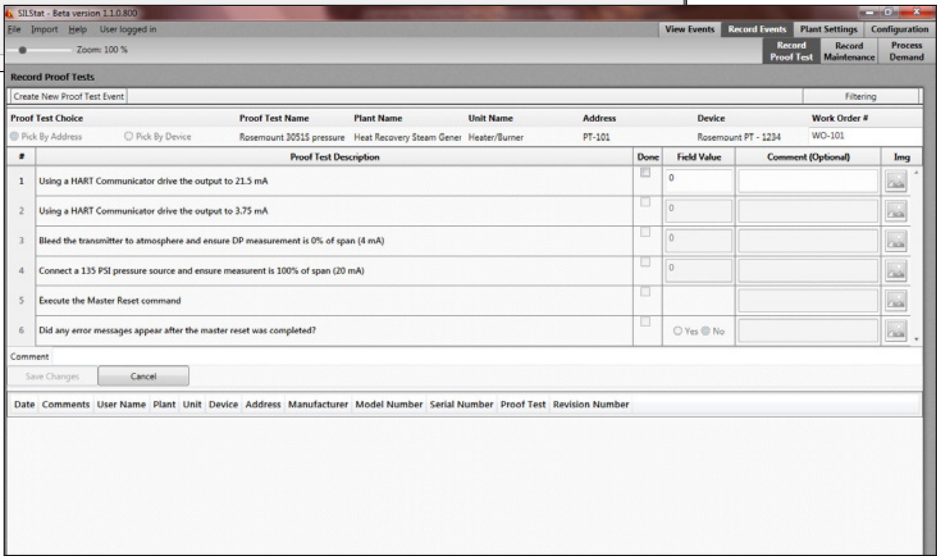
Revision Date: 11/4/2013

Revision Comments:

#	Proof Test Description	Field Type	Server Side Check
1	Bypass the safety function and take appropriate action to avoid a false trip.	None	N/A
2	De-energize the remote actuated valve, does the valve achieve the Fail-Safe state, is it completely closed?	Yes/No	● Yes ○ No
3	Energize the remote actuated valve, does the valve achieve the fully open position?	Yes/No	● Yes ○ No
4	Visually inspect the remote actuated valve elements. Are there any visible leaks? Is there any visual damage?	Yes/No	○ Yes ● No
5	Remove the bypass and otherwise restore normal operation.	None	N/A

Proof Test Name	Revision #	Revision Author	Revision Date	Revision Comment	Proof Test Active
Rosemount 3051S pressure transmitter			11/4/2013 2:18:36 PM		☑
ASCO 327 3-way Solenoid			11/4/2013 2:32:48 PM		☑
Bettis G-Series Actuator			11/4/2013 2:36:55 PM		☑
Flowserve Mark One standard trim			11/4/2013 2:39:41 PM		☑
Remote Actuated Valve close on trip			11/4/2013 2:43:17 PM		☑

Figure 8. Example template for a proof test generator.



Proof Test Choice		Proof Test Name	Plant Name	Unit Name	Address	Device	Work Order #
● Pick By Address	○ Pick By Device	Rosemount 3051S pressure	Heat Recovery Steam Gener	Heater/Burner	PT-101	Rosemount PT - 1234	WO-101

#	Proof Test Description	Done	Field Value	Comment (Optional)	Img
1	Using a HART Communicator drive the output to 21.5 mA	☐	0		
2	Using a HART Communicator drive the output to 3.75 mA	☐	0		
3	Bleed the transmitter to atmosphere and ensure DP measurement is 0% of span (4 mA)	☐	0		
4	Connect a 135 PSI pressure source and ensure measurent is 100% of span (20 mA)	☐	0		
5	Execute the Master Reset command	☐			
6	Did any error messages appear after the master reset was completed?	☐	○ Yes ● No		

Comment

Date	Comments	User Name	Plant	Unit	Device	Address	Manufacturer	Model Number	Serial Number	Proof Test	Revision Number

Figure 9. Example template for recording proof test results.

Essentially, being able to select and locate a device from the plant's hierarchy tree for maintenance and/or replacement via the tool will save time, especially if the O&M personnel can record the cause and any comments (figures 10 and 11).

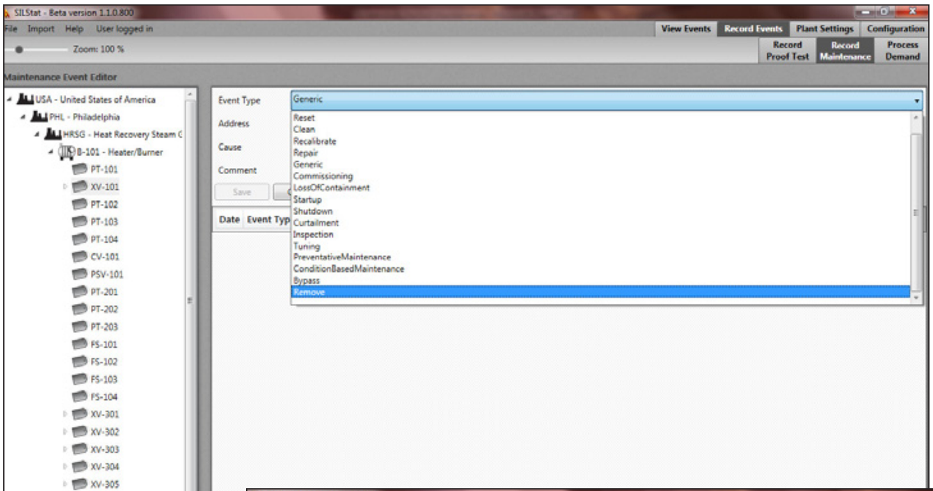
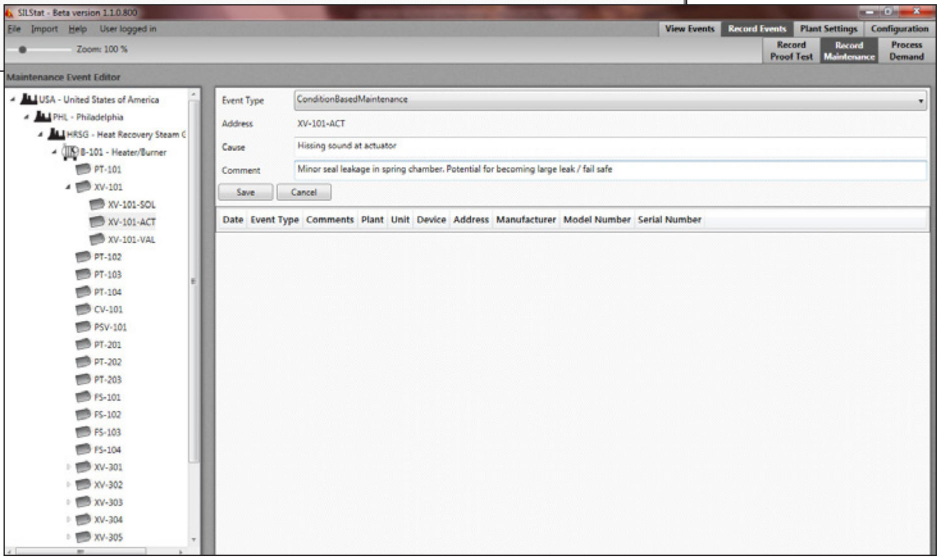


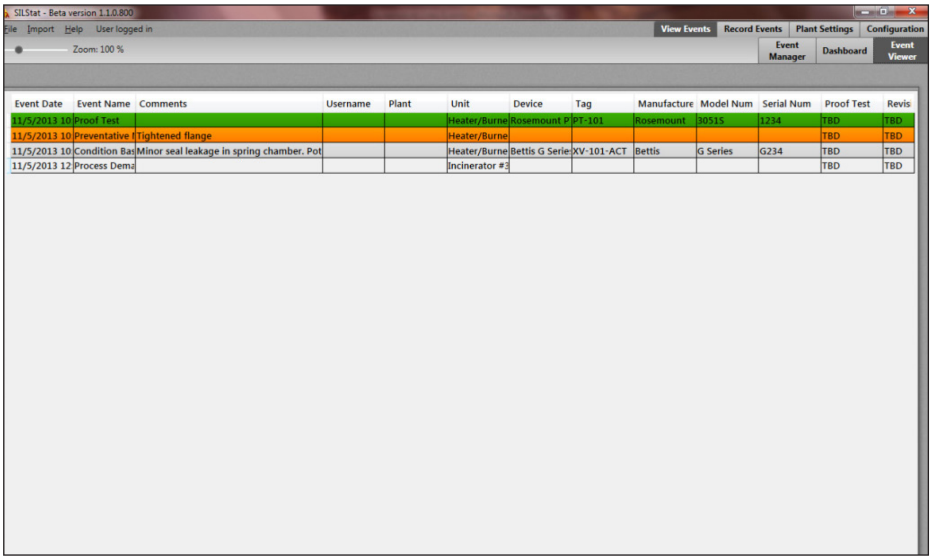
Figure 10. Example template for recording maintenance tasks.



Event Type: ConditionBasedMaintenance
Address: XV-101-ACT
Cause: Hissing sound at actuator
Comment: Minor seal leakage in spring chamber. Potential for becoming large leak / fail safe

Date	Event Type	Comments	Plant	Unit	Device	Address	Manufacturer	Model Number	Serial Number

Figure 11. Example template for recording maintenance tasks.



Event Date	Event Name	Comments	Username	Plant	Unit	Device	Tag	Manufacture	Model Num	Serial Num	Proof Test	Revis
11/5/2013 10	Proof Test				Heater/Burne	Rosemount P	PT-101	Rosemount	3051S	1234	TBD	TBD
11/5/2013 10	Preventative I	Tightened flange			Heater/Burne						TBD	TBD
11/5/2013 10	Condition Bas	Minor seal leakage in spring chamber. Pot			Heater/Burne	Bettis G Serie	XV-101-ACT	Bettis	G Series	G234	TBD	TBD
11/5/2013 12	Process Dema				Incinerator #3						TBD	TBD

Figure 12. Example template for displaying events.

Another benefit would be enhancing the ability of the O&M personnel and the plant's safety manager or team to view all the encountered events as presented in figure 12.

The benefits from maintenance of a well-structured, defined, and automated recording system include:

- detailed failure analysis
- false plant trip reduction
- comparison of actual performance with assumed performance
- adequate risk reduction
    - continued data collection
- ability to establish level of accuracy in risk reduction (high or low)
- the ability to identify if the risk reduction is more than adequate:
    - system is overdesigned
- enhance system flexibility
- data for future safety life-cycle tasks, including:
    - risk assessment
    - layer of protection analysis

- SIL target selection
- SIL verification.

The information gathered will enable the plant safety personnel to reevaluate the proof testing frequency based on the historical test data gathered, plant experience, hardware degradation, and software reliability subject to the plant safety manager.

In addition, a software tool can help solve any communication problems within the plant that exist between the various managers and their different departments.

Final thoughts

This article has outlined key issues involved in following the requirements of IEC 61511 Clause 16 for operation and maintenance of the SIS. As mentioned at the outset, the article highlights how testing and documenting the performance of an SIS is an essential part of ensuring it can fulfill its designed functional safety requirements, as defined in the SRS.

Key points include:

- There is a need to manage risk—not ignore it.
- There is a need to adopt an appropriate safety-first culture to ensure O&M personnel are trained and competent to maintain the plant SIS.
- Recording lagging and leading indicators is an important part of maintaining and improving process safety.
- Having the proper operation and maintenance procedures in place is vital to ensuring a safe and well-maintained SIS.
- Developing a safety checklist will ensure consistency in approach and methodology that can be adopted over multiple sites.
- Undertaking regular employee competency assessments is crucial to prevent mistakes that could lead to accidents or spurious plant trips.
- Ensure that proof testing is conducted in accordance with the safety requirements specification of the SIS (i.e., using the same test interval as used in the PFD_{avg} calculations).
- Recording all maintenance activities accurately and faithfully in accordance with IEC 61511 Clause 16.3.
- Using software tools/technology to assist in recording and auditing maintenance activities, spurious trips, SIS demands, calibration, and faults will save time and improve effectiveness.

- Using software tools/technology to help analyze failures, false trips, and actual performance of the SIS compared to assumed performance will help in meeting IEC 61511 Clause 16.2.6. Any discrepancies must be assessed.
- Well-recorded and accurate SIS performance data will enable plant safety personnel to reevaluate the frequency of proof testing, based on the historical data gathered, plant experience, hardware degradation, and software reliability.

ABOUT THE AUTHOR

Dr. Steve Gandy CFSP, DPE, MBA, DipM is vice president of global business development at exida. Gandy has more than 42 years of experience in hardware and software engineering for industrial controls and safety systems, pharmaceutical, and power utility applications. He currently leads the end user functional safety business for exida and is the lead trainer for the Functional Safety Engineering (FSE100) Course. Gandy has global business development responsibilities and provides support primarily to process industry end users in the areas of safety and security.

Related Articles

Case Study: Chemical Plant Safety System Features Advanced Coriolis Meters

The State of the Open Process Automation Standard (O-PAS)

Selecting the Best Control System for Automation Applications

Understanding Fire and Gas Systems Increases Safety

Risk Assessment: First Step to Securing an OT Environment

ASSURED AUTOMATION We Make **Valve Automation** Easy!

Thermal Shut-off Valves

FireChek®

Resettable Heat Activated Thermal Shut-off

an **Assured Automation**

Exclusive!

Adds Thermal Shutdown to ANY SIZE Spring Return Pneumatic Actuator!

- Vents actuator to fail-safe
- Shuts off supply air
- Easy to test and reset

Find Out More

Valves with Fusible Links

FM Fire-Safe Quarter-turn Valves

- NPT or ANSI Flange Ball Valves
- Butterfly Valves
- Optional Electric Remote Trigger
- 1/2” to 12” Line Sizes
- Various Trigger Temperatures

Find Out More

ESOV Swing Check Valves

- ANSI Flange Connections
- Optional Remote Triggers
- 2” to 16” Line Sizes
- Various Trigger Temperatures

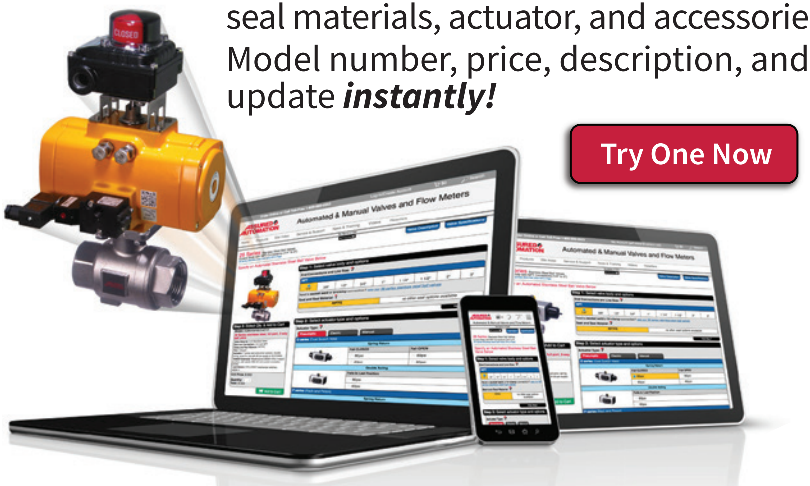
Find Out More

Try Our Easy to Use Actuated Valve Configurators

Build it, See it, Price it, Order it.

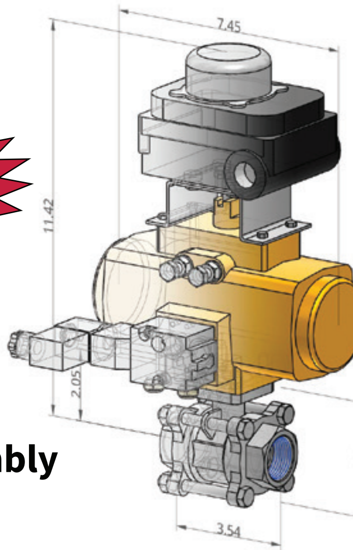
Point and click to specify valve type, end connections, seal materials, actuator, and accessories...
Model number, price, description, and photo all update ***instantly!***

Try One Now



NEW!

CAD Models & Datasheets
of the
Specified Valve Assembly
ON DEMAND!



assured**automation**.com

Closed-loop AI Enables Autonomous Process Manufacturing

Are we there yet? The move from automated to autonomous process manufacturing is right around the corner.

By Rajiv Anand, Quartic.ai

Figure 1. The autonomous plant of the future must be infinitely and continuously adaptive to deal with the change of flexible and resilient supply chains.

For process manufacturing, the ultimate promise of Industry 4.0 is autonomous manufacturing. Autonomous control of manufacturing processes is required, not to eliminate human workers, but to build resilient and highly responsive manufacturing supply chains. Resilience is required to enhance the top and bottom lines of a manufacturing enterprise.

The top-line drivers include the ability to introduce innovative, high-value, and high-margin new products to the market quickly. Consumerism as a trait of society is only going to increase. Our desire to live longer, healthier lives and to consume highly personalized products will continue to rise, making process manufacturing more complex.

The bottom-line drivers include the higher utilization of production assets for multiple products, waste reduction and recycling, and meeting energy and sustainability goals. This requires process manufacturing to be highly resilient. Resilience comes from flexibility.

Autonomous manufacturing, therefore, will need to be infinitely and continuously adaptive (figure 1). When and why is adaptability needed? Adaptability is needed when things change. So, if the manufacturing processes required for flexible and resilient supply chains will need to deal constantly with change, is the current state of automation sufficient?

Most of the concepts described in this article, which discusses the need for and opportunity of achieving autonomous manufacturing, refer to process manufacturing, with specific focus on batch/hybrid manufacturing. The underlying technology can extend to continuous and discrete manufacturing.

Opportunity versus current state

Process manufacturing has reached a state of high automation for the most part. Assume the manufacturing process is highly automated. This state of automation works well in a steady state and can deal with change usually in two forms: (1) transient states like startup, ramp up/down, and shutdown; and (2) variability caused by raw materials and process dynamics. Using advanced control and optimization, this state of automation also can handle changes in volume/capacity demand and from upstream process units.

Adaptive control is the capability of the system to modify its own operation to achieve the best possible operation mode. This requires the system to be able to perform the following functions: providing continuous information about the present system state or identifying the process (*observation*); comparing present system performance to the desired or optimal performance (*interpretation/analysis*); and making a decision (*decisioning*) to change the system to achieve the defined optimal performance (*action*).

Keep the term *system* in mind for the rest of this article. Also get familiar with the term *system-of-systems*. Assume a system to be a *unit operation system* as a minimum. A system-of-systems can be an entire supply chain consisting of multiple sites or plants—but for this article, assume it is a plant that consists of multiple unit operations.

For autonomous manufacturing at this plant, the system-of-systems will need to operate autonomously—without human intervention—to follow the changing commands from a management operating system (MOS) running the corporate manufacturing strategy execution.

> "To build an autonomous manufacturing system that can optimize systems or systems-of-systems, the system needs to observe, interpret, and make decisions on a much wider, zoomed-out view of the process, multiple process units, and the interactions among those units."

This cannot be done with the current state of automation, even with existing advanced process control/model predictive control (APC/MPC) and optimization. Heuristic-based expert systems have been used, and in some cases, provide limited success, generally at the unit operation level, if maintained and constantly updated.

But artificial intelligence (AI), specifically machine learning (ML), can get us there with closed-loop AI. And this is not in the far and distant future. We'll discuss how it is being done now and the rapid advances being made for its widespread use at scale. Some of the work being done by Quartic.ai is referenced in this article.

Is autonomous control of process manufacturing in sight?

Existing automation can handle regulatory controls, batch orchestration, and steady-state operations. It also can deal with transient states and upsets, and deal with variability and process dynamics at a loop and interactive loops with techniques like MPC.

But it is not autonomous.

To move from automated to autonomous, the following tasks being performed by humans—*at a system or system-of-systems level*—need to be automated: *observation, interpretation, decisioning, and action*. These are cognitive tasks that humans perform in the current state of automation in manufacturing. This is the essence of Industry 4.0 and autonomous manufacturing—automation of these cognitive tasks.

The generalized approach for achieving this can be treated as an optimization approach. If, when given a business command from the MOS, the system-of-systems (the plant) attempts to achieve an optimized state as quickly as possible, without causing any waste, off-spec product, cycle time loss, or energy loss, then it establishes the best mode of operation for underlying systems and automation (figure 2).

It must be assumed that the underlying systems can provide sufficient data (to inform) and are automated enough to be responsive to the commands—the plant must be sufficiently automated before it can become autonomous.

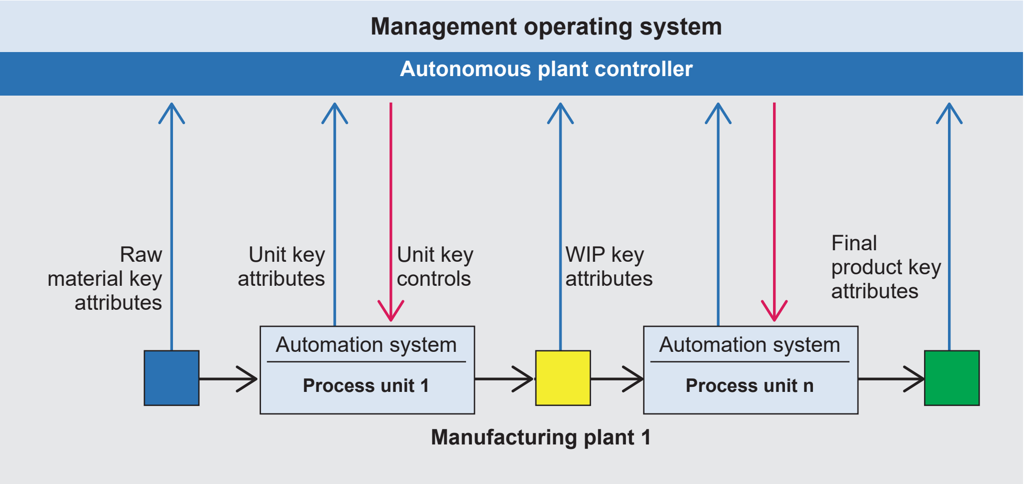


Figure 2. When given a business command from the MOS, the system-of-systems attempts to achieve an optimized state as quickly as possible, without causing waste, off-spec product, cycle time loss, or energy loss. It establishes the best mode of operation for underlying systems and automation.

The path to an autonomous manufacturing system goes through an optimization system. This optimization system will attempt to constantly optimize the objective(s) of the system-of-systems (plant), and in doing so, will generate commands and set points for the underlying systems.

MPC and EMPC

It is well understood that traditional MPC cannot be practically implemented at the system, let alone at a system-of-systems level. It does not directly optimize the end goal (e.g., profit, yield maximization). Instead, it just tries to track given set points. MPC has become a better substitute for proportional-integral-derivative (PID) controls in many cases.

To overcome the shortcomings of MPC, approaches like economic MPC (EMPC) were developed recently. EMPC removes the separation between optimization and control (e.g., it finds the optimal set points as well as the optimal way of tracking the set points), and can be used as a decision-making tool to achieve high-level goals directly. Could EMPC be used as this master controller to optimize, in real time, the objective function of a system or a system-of-systems?

EMPC has some key fundamental challenges even within the scope of the underlying systems it is being used for:

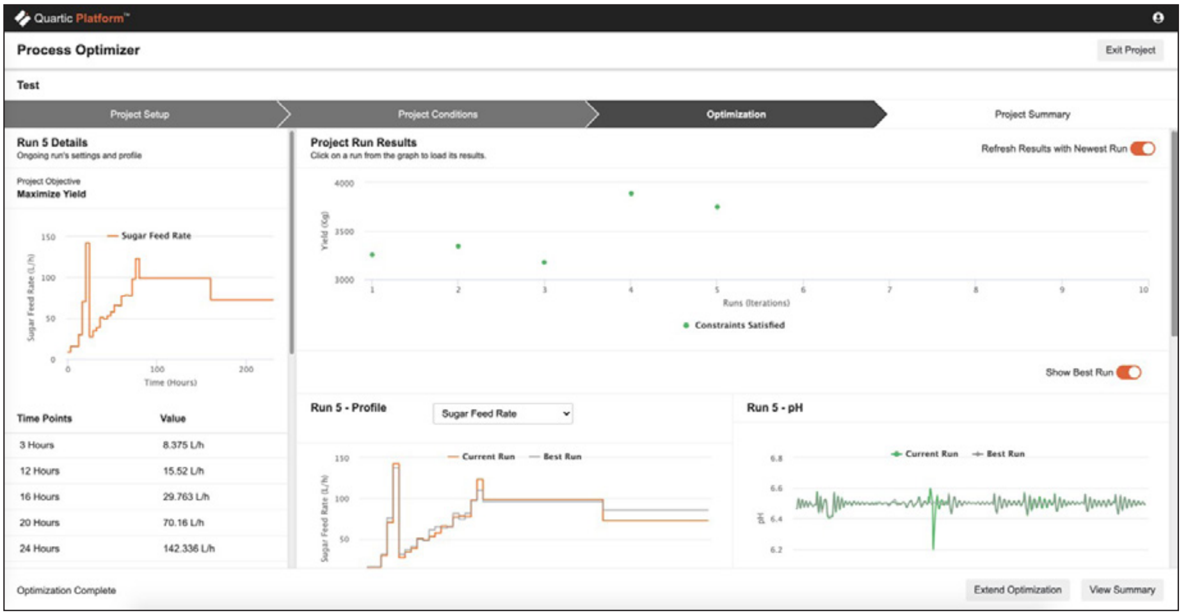
- A system model is required—whether it is a data-driven state-space model, a mechanistic model, or a combination of the two.
- Online computation load can be high, especially for nonlinear models. Depending on how the optimization is solved, sometimes a local optimum may not be achieved, which may lead to significant performance degradation (and instability).

To achieve an autonomous state, both of these challenges become highly amplified. Models will need to cover a much larger underlying process—multiple units, multiunit interactions, and combinations of serial and parallel processing units—in a flexible manufacturing realm for agile autonomous manufacturing. The computation load can become so high, in some cases, the compute cost may dilute the resulting benefits.

AI, ML, and closed-loop AI

Machine learning (sometimes in conjunction with underlying MPC) can be used as this system-of-systems optimizer in a closed loop or closed-loop AI. The mention of closed loop sometimes evokes existing mental models of what a loop is, and leads to apprehension and skepticism. The loop, in this context, is neither the traditional sensor-PID/MPC-actuator loop, nor is it the intention of AI to replace the PID loop. The loop in this context is either a system or ideally a system-of-systems.

Another mental model evoked, and the assumption made, is this loop must run at execution speeds of PID loops—and hence takes us to the hype about the use of AI at the edge—as if AI



Run 5 Details
Ongoing run's settings and profile

Project Objective
Maximize Yield

Time Points	Value
3 Hours	8.375 L/h
12 Hours	15.52 L/h
16 Hours	29.763 L/h
20 Hours	70.16 L/h
24 Hours	142.336 L/h

Project Run Results
Click on a run from the graph to load its results.

Run 5 - Profile

Run 5 - pH

Optimization Complete

Figure 3. If the loop is the system-of-systems, the execution requirements apply according to the dynamics of the entire plant and the frequency of the set-point demands from the MOS.

were to replace a flow control loop that is executing in milliseconds, and is highly synchronous with other loops. This is not the case, as it may be for an autonomous vehicle. If the loop is the system-of-systems (plant), the execution requirements apply according to the dynamics of the entire plant and the frequency of the set-point demands from the MOS (figure 3).

For manufacturing applications, ML and deep learning are being used successfully for anomaly detection, soft sensors, and forecasting (prediction). Predictive machine learning can be extended for some prescriptive (recommender) uses. However, since all ML algorithms are based on learning from co-relations, not causality, they cannot be used for optimization for autonomous manufacturing—to cause a change to achieve an optimal objective/outcome. Causal learning is in too early stages of research to be considered a viable option. To build highly accurate and responsive data science–based models, large historical informative training data sets must be built as well. ML algorithms need variance in the training data to learn from. This makes valuable training data even more scarce in manufacturing applications, particularly in industries like biomanufacturing where past data contains very little variance because processes are precisely controlled.

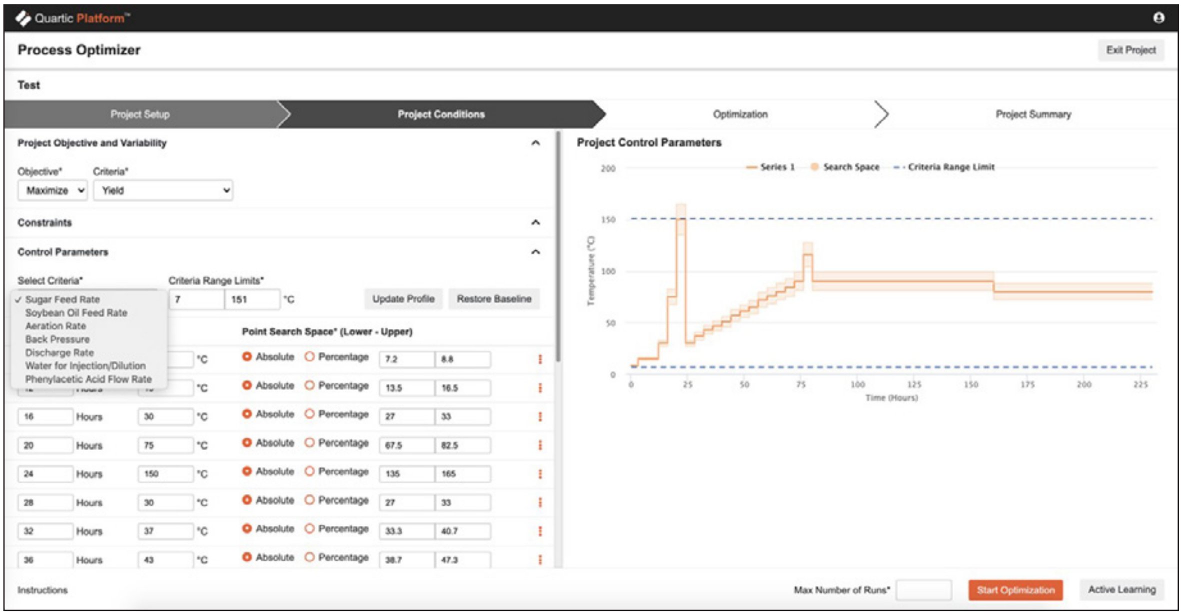
Deep reinforcement learning in conjunction with mechanistic models (hybrid learning) is also having some success, although in a limited way. The compute costs associated with deep reinforcement can be extremely high, and the high-fidelity mechanistic models are difficult and expensive to build, and in some cases, such as biological processes, near impossible (with current techniques).

We need techniques that can learn from little historical data (warm start), learn continuously, and cause changes (generate set points) to optimize.

Bayesian optimization

Rapid progress can be made with Bayesian optimization. Bayesian optimization can be used to optimize any black-box function. A black box function is a function where the relationship between inputs and outputs cannot be easily represented mathematically or are vague, but the effects on the output can be observed. For manufacturing applications, where high-fidelity mechanistic models cannot be built, a black box builds a surrogate for the objective and quantifies the uncertainty in that surrogate using a Bayesian machine learning technique, Gaussian process regression. It then uses an acquisition function defined from this surrogate to decide where to sample. Bayesian optimization is an ideal approach to optimizing objective functions that take a long time (minutes or hours) to evaluate.

This technique was used successfully for batch process optimization of a fed-batch fermentation bioreactor (figure 4). With only set-point measurements and the final objective function (yield), the Bayesian optimizer could achieve a 4 percent average yield increase with 400 batch runs of optimization. No process parameter measurements were used in the process. The optimizer can be used for a cold start (only starting set points from the recipe/work instruction are used), a warm start (known ideal set points are available from previous batch runs), or online learning (the optimizer uses the starting set points and continually learns and optimizes). The continuous/online learning mode is ideal for closed loop/autonomous control and is being used for a continuous chemical reactor.



Objective*: Maximize

Criteria*: Yield

Select Criteria*: Sugar Feed Rate

Criteria Range Limits*: 7 – 151 °C

				Point Search Space* (Lower - Upper)		
			°C	● Absolute ○ Percentage	7.2	8.8
	Hours		°C	● Absolute ○ Percentage	13.5	16.5
16	Hours	30	°C	● Absolute ○ Percentage	27	33
20	Hours	75	°C	● Absolute ○ Percentage	67.5	82.5
24	Hours	150	°C	● Absolute ○ Percentage	135	165
28	Hours	30	°C	● Absolute ○ Percentage	27	33
32	Hours	37	°C	● Absolute ○ Percentage	33.3	40.7
36	Hours	43	°C	● Absolute ○ Percentage	38.7	47.3

Max Number of Runs*:

Figure 4. Bayesian optimization is an ideal approach to optimizing objective functions that take a long time (minutes or hours) to evaluate. This technique has been used successfully for batch process optimization of a fed-batch fermentation bioreactor.

Further optimization can be achieved when process measurements, including a good, online measurement of the objective function, are available, and a high-fidelity model (digital twin) is used in conjunction with the ML optimization. Using Raman spectral data for online measurement of the yield, the system was able to achieve approximately 10 percent performance gain on average for 100 batches.

To build an autonomous manufacturing system that can optimize systems or systems-of-systems, the system needs to observe, interpret, and make decisions on a much wider, zoomed-out view of the process, multiple process units, and the interactions among those units. This level of analysis cannot be handled by existing control and optimization techniques; it becomes a big data control problem to solve. Machine learning, combined with mechanistic models and MPC, provides a path toward real-time, continuous optimization, with which autonomous manufacturing can be built.

All figures courtesy of Quartic.ai

ABOUT THE AUTHOR

Rajiv Anand is the cofounder and CEO of Quartic.ai. He is an instrumentation and control engineer with 30 years of experience implementing process control and asset health solutions for power, mining, pharmaceutical, and chemical industries.

Related Articles

Digitalization will accelerate, pushing manufacturers to transform and enabling innovation

The evolving era of AI in all its forms is driving industrial transformation today

Connected applications: When IIoT meets software

At John Deere, ‘Hard Iron Meets Artificial Intelligence’

How AI Can Help the Food Industry Address Two of its Biggest Expenses

Manufacturers Urged to Consider Best Practices for Optimizing Control Plans with AI

3 Use Cases that Show How to Bring Your Industrial AI Strategy to Life

Rethinking Operational AI

ISA GLOBAL CYBERSECURITY ALLIANCE

THE TIME IS NOW

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

The ISA Global Cybersecurity Alliance is an open, collaborative body.
We welcome members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Founding Members:

Honeywell
Johnson Controls
Rockwell Automation
Life Is On Schneider Electric
NOZOMI NETWORKS
PAS
CLAROTY Clarity for OT Networks
WALLIX CYBERSECURITY SIMPLIFIED
xage SECURITY
MOCANA
BAYSHORE
radiflow Secure your Assets
senhasegura by MT4 Technology
INL Idaho National Laboratory
威努特 WINICSSEC
exida
munio security
tenable
DRAGOS
TiSafe
ae Solutions
tripwire
DIGITAL IMMUNITY STAY PRODUCTIVE, STAY SECURE
WisePlant Smart, Safe & Secure
MSi Mission Secure, Inc.
1898 & Co.
ACET SOLUTIONS
CYBEROWL
Nova Systems

International Society of Automation
Setting the Standard for Automation™

PETRONAS Upstream Improves Operational Performance

By Mark Carrigan, PAS

Case Study: PETRONAS achieves operational performance through digital transformation and collaboration.

Modern process plants across industries such as oil and gas, chemicals, metals and mining, and power generation are highly automated. A variety of technologies including distributed control systems (DCSs), advanced process control (APC), safety instrumented systems (SISs), and emergency shutdown systems (ESDs) help ensure reliable, safe, and economic process operations. The typical plant invests millions of dollars in acquiring such systems and maintaining them over a lifespan that can run into two or three decades.

However, plant owners cannot take a fit-and-forget approach to their process automation systems. Rather, these need to be managed astutely and supplemented appropriately to ensure that process operations are not compromised, either when operation staff is on site or when they are monitoring and managing a site from a remote location. Issues and problems that can arise include: an excessive and unnecessarily high number of generated process alarms that control room operators cannot address adequately; poor visibility into the extent of SIS bypass activations that can make a facility vulnerable to process safety incidents from disabled safety instrumented functions; and inefficiently and incorrectly running control loops, which can have multiple negative impacts, including economic loss from poor quality product and increased operator interventions and workload.

Against this backdrop, ARC Advisory Group met with executives from Petroliam Nasional Berhad (PETRONAS), the national oil and gas company of Malaysia, to discuss its strategic initiative for operational excellence, digitalization, and remote operations—code named PRIME Solutions. This initiative leverages the implementation of PAS PlantSuite Integrity across multiple sites in upstream oil and gas production operations. While the implementation is a continuing, multiyear endeavor, the results from the first installations in Malaysia point to significant gains in operational performance, an increased ability to monitor and drive operations remotely, and the achievement of specific objectives related to improved process safety, reliability, and cost-effective process operations.

PETRONAS Upstream business

Along with the Downstream division and the Gas and New Energy division, Upstream is one of the three major operating divisions of PETRONAS. Onshore and offshore exploration and production of oil and gas takes place not only in its home territory but in more than 20 other countries around the world, including Angola, Argentina, Australia, Canada, Gambia, Indonesia, Iraq, Myanmar, and Turkmenistan.

In the 2019 financial year (ending 31 December), the Upstream business reported revenues of RM 102.6 billion (U.S. $23.6 billion) and profit after tax of RM 22.2 billion. Other pertinent data for the segment includes: 233 producing fields, 419 offshore platforms, 29 floating facilities, and more than 12,000 staff members.

As with all oil and gas companies hit hard by the oil price crash in the middle of the last decade, PETRONAS was forced to evaluate and retool its business strategies for an era in which consistent and easy profits could no longer be guaranteed by prices of more than $100 for a barrel of oil, and in which regulators and society would pay much greater attention to activity and performance in the area of health, safety, and environment.

> "Initial results from a multiyear progressive implementation at 37 PETRONAS oil and gas facilities in Malaysia point to the achievement of significant improvement gains in the aspects of process safety, reliability, and cost-effective process operations."

In the 2016 annual report, PETRONAS Upstream emphasized its focus on reducing costs and delivering projects with discipline, but also, and significantly, on the need to prioritize safety and asset integrity. The latter aspects were reiterated in the 2017 review when the executive vice president and CEO of the Upstream division stressed the need to "continue to focus on value-driven growth and improve our operational excellence to ensure safety, reliability, and sustainability of the business."

UPSTREAM

- Prioritize safety and asset integrity
- Prioritize margins over production volume via cost reduction initiatives
- Maximize value of integrated domestic production across the value chain
- Secure new LNG customers
- Maintain consistent investment in exploration to support future growth

Figure 1. Prioritizing safety and integrity is a key strategic objective for PETRONAS Upstream
Source: PETRONAS Annual Report 2016

The PRIME Initiative

The more demanding external environment and renewed corporate focus on operational excellence, remote monitoring, and digitalization led to the development of the PRIME Initiative at PETRONAS Upstream. An acronym for "predictive revitalization of instrument to maximize efficiency," PRIME focuses on three aspects of plant operations at Upstream's onshore and offshore installations: safety—improving process safety performance; reliability—improving process control performance; and cost efficiency—improving risk management performance.

Figure 2. PRIME focus: improve safety, reliability, and cost effectiveness of PETRONAS Upstream operations
Source: PETRONAS

These three together also help satisfy the objective of developing a collaborative new way of working, something important and valuable for the Upstream division, given the geographically dispersed and often remote nature of its operations. With different sites having different operating practices, the PRIME program is an opportunity to standardize efficient and effective processes across all Upstream facilities.

Responsibility for the development and realization of the PRIME program is with the operational excellence department within the Upstream Center of Excellence (CoE) located at PETRONAS headquarters in Kuala Lumpur. The CoE provides the necessary expertise and strategic, operational, and technical support by remotely monitoring and engaging with on-site and off-site staff at the various Upstream production sites.

The initiative was conceptualized, developed, and refined during 2016. This was followed by multiple engagement and communication sessions on PRIME plans and objectives to various stakeholders including senior executives and Upstream facilities' personnel to promote awareness and buy-in and secure budget allocation. The request for proposals, tender bid evaluation, and selection process took place over a lengthy 10 months in 2017.

> "The analytical and visualization capabilities of PlantState Integrity increase awareness and understanding of operations, enhance collaboration, and facilitate the deployment of common best practices across multiple PETRONAS Upstream sites."

Technological and commercial assessment ranked suppliers that could satisfy the PRIME objectives of improving the safety, reliability, and cost effectiveness of Upstream plant operations, including the provision of remote monitoring with comprehensive dashboards. With an eye toward expediting the implementation timeline by eliminating the need to deploy multiple point solutions and avoid potential data integration issues, PAS' single-suite approach was a major plus point in the eventual selection of PlantState Integrity.

Introducing integrity

PlantState Integrity is a modular product that offers a suite of solutions designed to ensure safe, reliable, and cost-effective industrial operations. These solutions address problems commonly faced in process facilities, such as alarms generated at such a frequency that they that cannot be effectively handled by operators, inadequate control and management of safety function bypasses, an unnecessarily high number of control loops in manual mode or in saturation, and operating and safety limits set outside of designed boundaries.

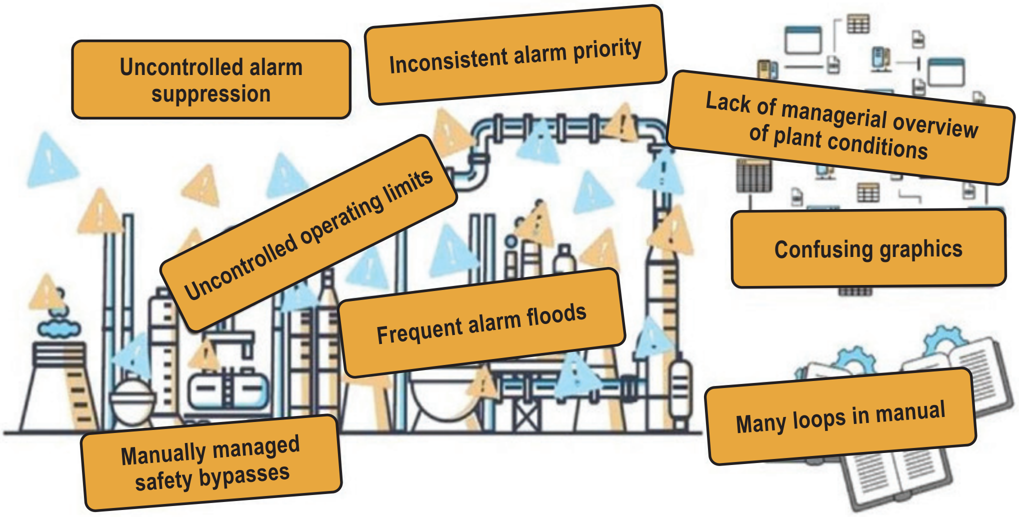


Figure 3. Issues that can affect plant operational performance
Source: PAS

The first phase of the project, designated PRIME 1.0, involves deployment across a planned 37 Upstream sites. For this phase, PETRONAS is implementing four PlantState Integrity modules that functionally address alarm management, safety life-cycle management, control loop performance, and operating boundary management.

Alarm management

In the market research study on alarm management published in 2019, "Alarm Management for the Process Industries Market Analysis," ARC notes the generally poor state of alarm management in process plants. The primary contributor is the sheer number of alarms generated per shift, which prevents control room operators from making timely and effective intervention. The main cause of all those alarms is the negligible cost of implementing alarm points with a modern DCS, which means designers have no disincentive to adding yet another alarm to the P&ID configuration.

It is thus important for plants to have an alarm management strategy in place so operators and CoE personnel have the right information to quickly recognize and respond to abnormal situations. This can only be accomplished if they are not overwhelmed by spurious alarms that cause distractions and reduce situational awareness.

To aid end users in this regard, the ISA-18.2 (IEC 62682) industry standard provides a framework for implementing an effective and sustainable alarm management strategy in process plants. It prescribes a life cycle–based approach to alarm management in which alarms are set up, rationalized in a consistent way, and reviewed for effectiveness.

Alarm management software such as the kind available through PlantState Integrity, can help facilitate implementing ISA-18.2-compliant best practices in the plant. This solution caters to key ISA-18.2 aspects, including developing and documenting the alarm philosophy; rationalizing alarms; and alarm monitoring, analysis, and auditing. ARC recommends that end users adopt alarm management software that conforms to the ISA-18.2 standard.

Another key ARC recommendation for end users like PETRONAS is that independent (i.e., non-DCS supplier) alarm management software should tightly integrate to a variety of distributed control systems. Given the heterogeneous nature of DCS installations across PETRONAS Upstream, the capability of PlantState Integrity to support multivendor DCS environments was another important consideration in its selection as the alarm dashboard (PRIME-ADB) in the PRIME project.

Safety life-cycle management

To ensure process safety and prevent the type of mass casualties that can potentially occur, notably in the hydrocarbon-based industries, owner/operators commonly implement a safety instrumented system. However, to be effective, the SIS must be managed properly throughout its life cycle, i.e., from initial concept and requirements definition to in-plant operation, maintenance, modification, and finally, decommissioning.

A particularly challenging aspect of the safety life cycle is operations and maintenance. SIS design information and safety procedures are often kept in disparate spreadsheets and documents, such that actual operation of the safety system can evolve away from the design intention without it becoming apparent.

There also is often inadequate analysis and hence understanding of safety instrumented function (SIF) activations and SIF bypass activations. While it is often necessary to bypass an SIF during plant upset, startup, SIS testing, and other non-steady-state events, poor record keeping of these actions can mean safety functions are disabled for much longer than intended, potentially compromising safety.

Adoption of software technology that helps industrial end users better manage the safety life cycle is becoming more prevalent. ARC forecasts a significant growth in revenues for life-cycle management software over the next five years, as more companies acknowledge the importance of meeting regulatory requirements and adhering to industry standards and best practices.

Implemented as PRIME-IPM in the PRIME project, PlantState Integrity's safety life-cycle management module (IPL Assurance) is helping PETRONAS Upstream ensure effective safety instrumented function management at its installations with on-site and remote monitoring. This reduces the risk of a serious process safety incident. A particularly notable result is the ability to track when safety functions are bypassed, by whom, and for how long. Previously bypassed safety functions were not tracked effectively, leading to increased risk. With the PRIME-IPM solution in place, this is no longer the case.

Control loop performance management

Safe, reliable, and cost-effective industrial operations depend on the proper functioning of the thousands of control loops running in the typical process facility. Poor control loop performance can be caused by mechanical wear of control valves, compressor fouling, and neglecting to retune for process changes. The consequences can include an inordinately high number of loops placed in manual control, unnecessary alarm generation, and negative impacts on production output and quality.

PlantState Integrity (i.e., PRIME-CLP in PRIME Project) provides on-site and remote management of control loop performance by continuously monitoring, analyzing, and diagnosing the functioning of control loops. Particularly useful for operators is its ability to prioritize loop performance issues; identify possible contributing issues with controllers, valves or sensors; and recommend corrective actions. With PRIME-CLP, control loop performance is systematically analyzed, tracked, and managed for better process control in general.

Operating boundary management

In process plant operations, it is important that process boundaries are specified, documented adequately, and monitored for any excursions. These boundaries include limits for operating zones, i.e., optimal, acceptable, alarmed, for safety system trips, and for equipment mechanical operation. This information is often kept in different databases and locations, which can make it hard to access and control.

PRIME-ADB
Alarm Dash-Boarding & Performance Analysis
- Real-time alarm management and governance
- Alarm management benchmarking and performance across the operating fields through aggregation of alarm analytics, reporting and metrics for identification of problem areas to drive improvements

PRIME-ODM
Operation Deviation Management (SOL/Operating Envelope/PSM)
- Real-time monitoring of plant's safe operating limits (SOL), safe operating envelope and proximity of the current operating point for performance optimization, safety/integrity assurance
- OEMS compliance support
- Automatic alerts and notifications

PRIME-IPM
IPF Performance Management
- Real-time (MOS) bypass governance
- Provides capability to deliver accurate, real-time IPF performance assurance & validation with reporting and analytics

PRIME-CLP
Control Loop Performance Management
- Regulatory control loop performance assessment tool
- Analyze all control loop elements for root cause i.e. sensor, controller & control valve and rank close loop in order of performance
- Recommend corrective actions
- Controller diagnostic and tuning

Figure 4. The PRIME implementation of PAS PlantState Integrity
Source: PETRONAS

Boundary management software gives plants a single repository for boundary limit data along with logical visualization. Personnel are alerted automatically to deviations from designated boundary limits. With PlantState Integrity, both on-site operation teams and CoE personnel at PETRONAS Upstream can visualize all the critical operating parameters and safe operating limits on a process safety dashboard with reports on violations. For example, detecting a pump low-pressure alarm set to a value lower than the pump trip can help avoid a costly process shutdown.

Realizing PRIME value

The PRIME project and implementation of PlantSuite Integrity was still ongoing as of mid-2020, but PETRONAS was already seeing positive results and value creation from its investment in the software solution. For example, at one plant, the new alarm management capability has led to an almost 90 percent reduction in alarm rates, with average alarms per hour per operator falling from 44.5 to 5.6. As well as a clear operator efficiency gain, PETRONAS executives appreciate that an effective alarm management system translates to a real reduction in process safety risk, as critical situations are far more likely to get priority for any necessary remedial action.

Also contributing to improved process safety is the marked reduction of unnecessary SIF bypasses, which fell from 101 to just seven at one offshore platform after the implementation. PRIME-IPM also facilitates the bypass governance model, which PETRONAS Upstream has introduced for a procedural rather than the previously somewhat ad-hoc approach to activating, monitoring, and deactivating safety bypasses.

Meanwhile, with control loop performance management, PETRONAS Upstream is getting highly useful dashboard visibility into control loop elements such as the status of control valves out in the field. For example, the PRIME solution identifies valves that are cycling too frequently, sticking, or are oversized for the process. This information was previously unavailable without running time-consuming control valve tests.

Remote operations visualization is a powerful and, indeed, striking aspect of PRIME. On large display dashboards at the CoE Petronas Digital Collaboration Center (PDCC) area at PETRONAS HQ, hundreds of miles away from the terminals and platforms, the staff gains insight into what is happening (across the four PRIME Solutions) at all those facilities in real time. While each facility also has a PRIME dashboard for insights on its own performance, data analysts at PDCC/HQ prepare weekly reports. These are made available to the facilities for discussion and improvement actions.

Initially, and perhaps not surprisingly, there was concern from individual plants on exposing their operations in this way. In one instance, a plant manager was surprised to be informed by the operational excellence team at HQ of an inordinately large number of safety bypasses activated at his facility. But he took it positively and worked together with the HQ team to reduce the bypasses to help lower the safety risk at the facility. Having all-round visibility on the activities and performance at multiple and often very remote sites allows PETRONAS Upstream to work toward its goal of instilling common best practices and improving collaboration.

Looking ahead

The current turbulence in oil prices along with the economic fallout from the COVID-19 situation increases the imperative for oil and gas and other heavy process industry companies to relentlessly seek improvement opportunities that ultimately translate positively to the business bottom line. Taking a methodical and structured approach with its operational excellence, digitalization, and remote operations, PRIME project, PETRONAS Upstream is reaping significant gains across process safety, reliability, and cost efficiency to help meet broader corporate objectives for business profitability and sustainability.

The increasing sophistication and ease of use of digital tools such as PlantState Integrity, adopted by PETRONAS as the technological enabler for the ambitious PRIME project, facilitate opportunities for companies to make such improvements. In addition to driving marked improvements in alarm management and control loop performance, the analytical and visualization capabilities of PlantState Integrity (PRIME Solutions in PETRONAS) increased awareness and understanding of operations, enhanced collaboration, and facilitated the deployment of common best practices across multiple sites.

In PRIME 2.0, PETRONAS Upstream is also planning to deploy additional capabilities with PAS Cyber Integrity. The objective is to boost protection against industrial cybersecurity threats and further improve operating integrity and performance of its oil and gas production facilities.

ABOUT THE AUTHOR

Mark Carrigan is chief operating officer and chief revenue officer at PAS, where he has worked since 2000. He leads the technology, operations, and sales organizations. During his tenure at PAS, Carrigan has held a variety of positions including senior vice president of technology, managing director for the Middle East, and global sales leader. He has extensive experience in international business, engineering, sales, and technical consulting in the processing industries.

Related Articles

The Perfect Downtime Storm is Brewing for Oil and Gas Companies this Summer

Digital transformation: Getting started, accelerating quickly

Unlocking the Benefits of the IIoT in the US

Supply Chain Management with Digital Transformation

Industrial Digital Transformation Made Easy with MQTT

Digitalization in Service and Maintenance: Process Industry in Transition

Essential Digital Twins for Upstream Oil and Gas Production Operations

ISA95 In the IoT & Digitalization Era

Automatic Configuration of a Safety Instrumented System

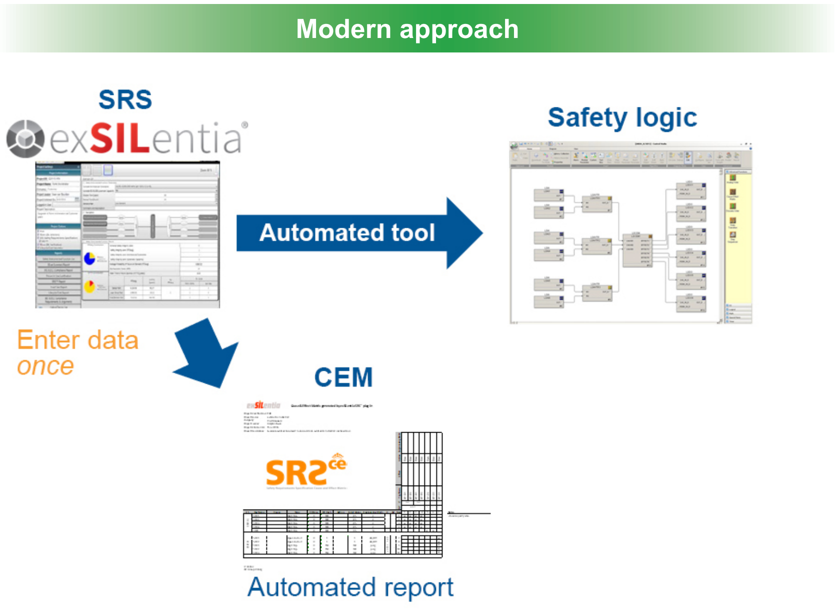
By Sergio Diaz, Emerson

The DeltaV SIS Configurator tool can provide a consistent approach with fewer errors and less rework.

Safety instrumented systems (SISs) have traditionally been configured manually using different source documents such as the safety requirement specification (SRS), cause and effect matrices (CEMs), safety integrity level (SIL) calculations, and I/O definitions, among other information.

Emerson partnered with exida to deliver a database-based solution that enables automatic configuration of safety logic using information captured in exida's exSILentia software suite. An evident advantage of this approach is the reduced configuration effort. However, the real benefit is having a consistent configuration approach that has fewer errors and less rework and that is easily traceable back to the SRS.

The DeltaV SIS Configurator tools provide great benefits for the implementation of emergency shutdown (ESD) projects within DeltaV safety instrumented systems. While the exSILentia tool does not generate the full DeltaV SIS configuration, it can potentially generate up to 90 percent of the safety



Emerson partnered with exida to deliver a database-based solution that enables automatic configuration of safety logic using information captured in exida's exSILentia software suite.

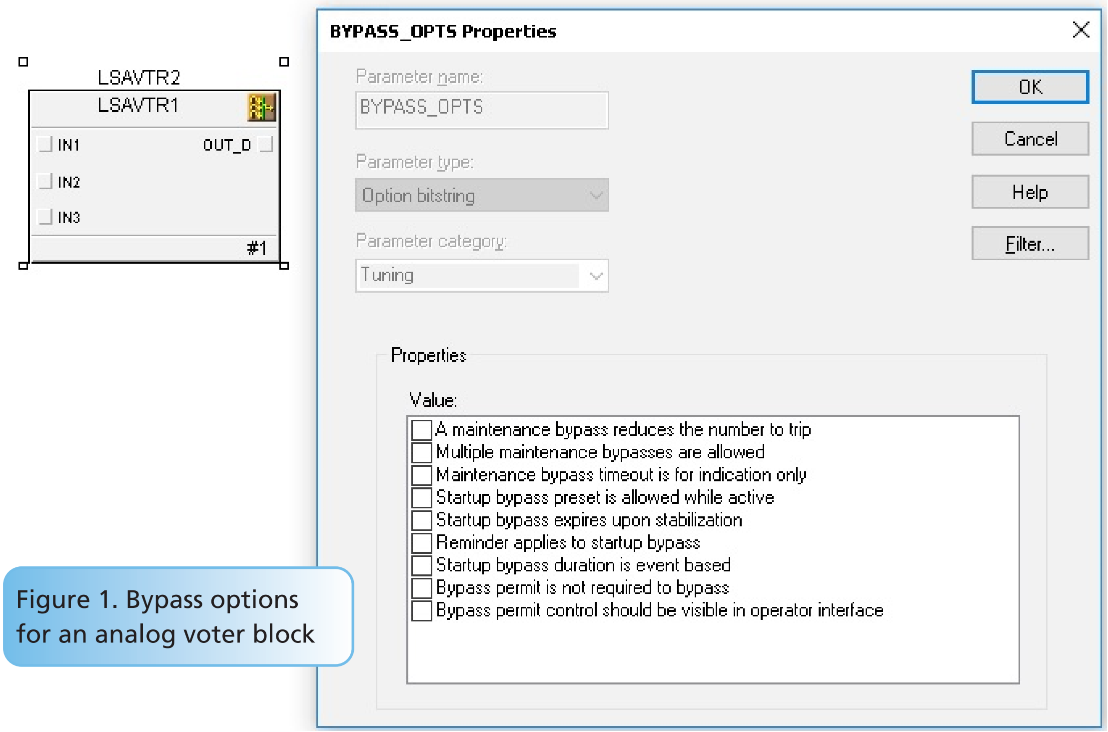
logic. The user still needs to create input/output (I/O) configuration, graphics, and alarms. In addition to the time savings, another benefit is a consistent approach with less error.

This article is a high-level overview of the capabilities of the DeltaV SIS Configurator developed by exida. It is not intended as a configuration guideline. For further details please refer to exida's documentation (*exSILentia User Guide* and *DeltaV SIS Configurator User Guide*).

DeltaV SIS configuration overview

The DeltaV SIS process safety system makes configuration of safety instrumented functions (SIFs) easy. The DeltaV SIS built-for-purpose function blocks can help to eliminate engineering hours required to implement safety applications. The TÜV-certified function blocks deliver powerful functionality out of the box, simplifying the implementation of complex SIS applications.

One of the advanced function blocks is the analog voter function block, which has advanced features to easily implement "M" out of "N" voter functions. That is, "M" inputs of the total "N" inputs must vote to trip. For example, the block can be configured as a 2oo3 (two out of three) voter, where two of the three inputs must exceed the trip limit before the output is tripped. What used to take a fair amount of programming using "AND" and "OR" logical gates is now replaced by a standard function block configured using radio buttons and check boxes (figure 1). For example, if the application needs to prevent multiple maintenance bypasses at the same time, the user only needs to check one box. If the application requires a bypass timeout to either automatically remove the bypass after a predefined time or simplify to provide an alert, the user again just needs to select the proper options within the bypass option parameter.



BYPASS_OPTS Properties

Parameter name: BYPASS_OPTS

Parameter type: Option bitstring

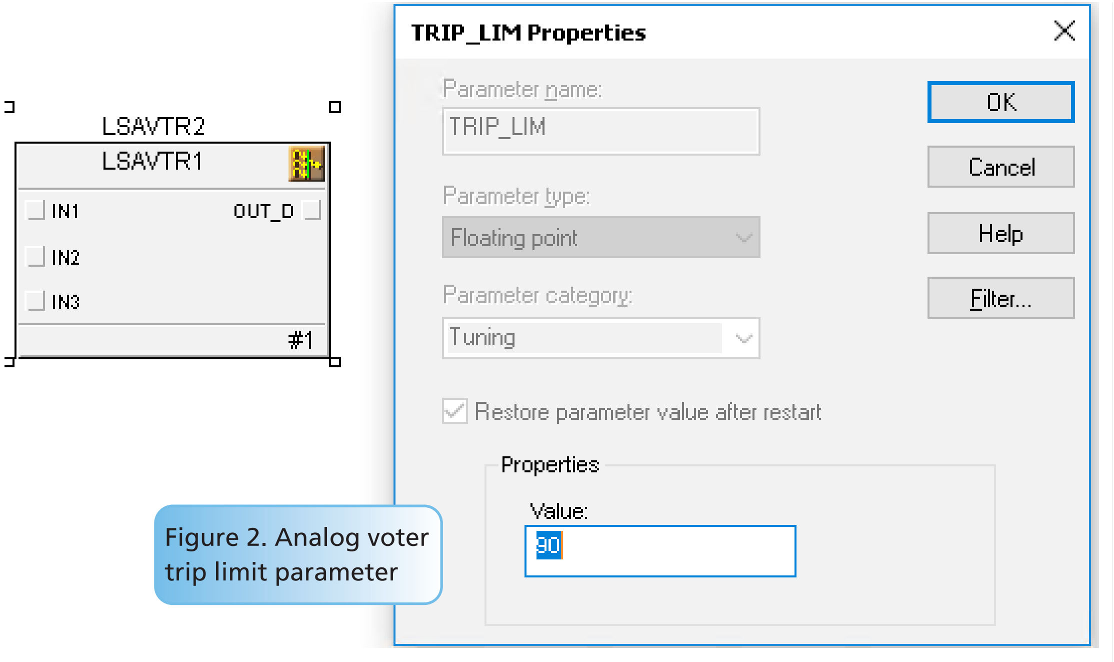
Parameter category: Tuning

Properties

Value:

☐ A maintenance bypass reduces the number to trip
☐ Multiple maintenance bypasses are allowed
☐ Maintenance bypass timeout is for indication only
☐ Startup bypass preset is allowed while active
☐ Startup bypass expires upon stabilization
☐ Reminder applies to startup bypass
☐ Startup bypass duration is event based
☐ Bypass permit is not required to bypass
☐ Bypass permit control should be visible in operator interface

Figure 1. Bypass options for an analog voter block



Parameter name: TRIP_LIM

Parameter type: Floating point

Parameter category: Tuning

☑ Restore parameter value after restart

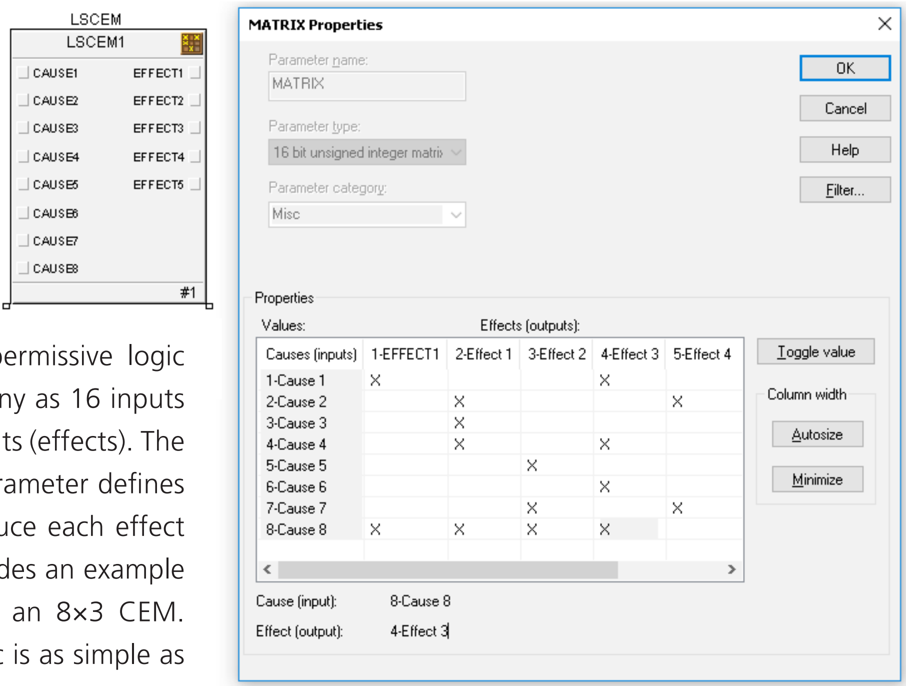
Value: 90

Figure 2. Analog voter trip limit parameter

Trip limits, trip delays, and detection types (high limit or low limit) are easily configured using parameters (figure 2).

All the traditional programming required for implementing an analog voting function has been replaced by a few configuration settings. In the same way, there is a discrete voter function block with similar functionality.

Implementing a cause-and-effect relationship is done using another advanced function block. The cause-and-effect matrix function block defines interlock and permissive logic that associates as many as 16 inputs (causes) and 16 outputs (effects). The block's "MATRIX" parameter defines the causes that produce each effect to trip. Figure 3 provides an example of how to configure an 8×3 CEM. Defining the trip logic is as simple as selecting the proper intersections in the "MATRIX" parameter.



Parameter name: MATRIX

Parameter type: 16 bit unsigned integer matri

Parameter category: Misc

Values:

Effects (outputs):

Causes (inputs)	1-EFFECT1	2-Effect 1	3-Effect 2	4-Effect 3	5-Effect 4
1-Cause 1	X			X	
2-Cause 2		X			X
3-Cause 3		X			
4-Cause 4		X		X	
5-Cause 5			X		
6-Cause 6				X	
7-Cause 7			X		X
8-Cause 8	X	X	X	X	

Cause (input): 8-Cause 8

Effect (output): 4-Effect 3

Figure 3. CEM block matrix parameter

Although a 16×16 matrix might seem relatively small, the reality is that DeltaV SIS breaks the configuration in SIFs, and the need for large matrices is greatly reduced. While the overall project CEM might include hundreds of causes and hundreds of effects, individual SIFs typically do not have more than 16 causes or 16 effects. Most of the SIFs can be implemented using the CEM function block. For the few SIFs requiring larger matrices, DeltaV v14 introduced two new function blocks ("MONITOR" function block and "EFFECT" function block). There is no set limit for the number of causes or effects that can be implemented combining the new "MONITOR" and "EFFECT" blocks.

SIF configuration

Implementing a SIF in DeltaV SIS is quite simple (figure 4):

1. Drag and drop the proper function blocks.
2. Wire the function blocks as appropriate.
3. Configure the proper parameters.

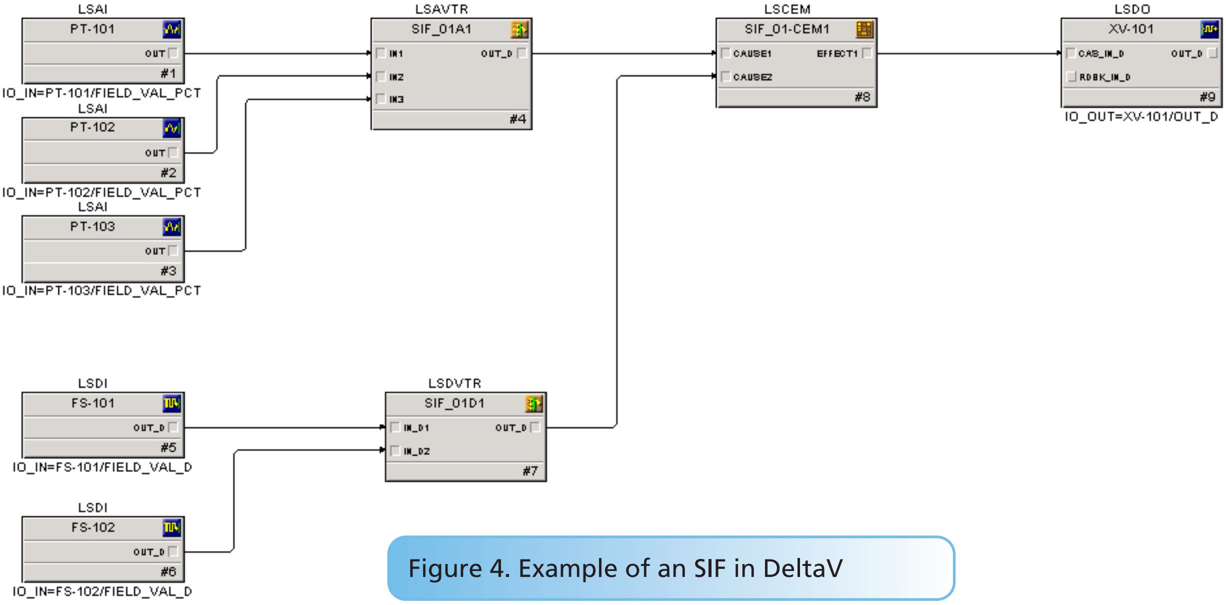


Figure 4. Example of an SIF in DeltaV

Applicability of the DeltaV SIS Configurator

The ability to automatically generate DeltaV SIS safety logic is based on a sound conceptual design using exSILentia. An incomplete SRS will not generate the expected results. DeltaV-relevant information (e.g., signal tags) needs to conform with DeltaV syntax. The DeltaV SIS Configurator tool generates proper warning messages when the DeltaV SIS syntax rules are not being followed, and in most cases, the log file provides sufficient indication for resolving the issue.

The use of the DeltaV SIS Configurator does not eliminate proper engineering practices. In fact, a more structured approach is needed. Configuration implementation should not start until the design SRS is finalized and all relevant information for the DeltaV SIS is properly captured. Only users who have used exSILentia as both an SRS compilation tool and an SIL calculation tool will benefit from this solution. There are no migration tools to take SRS or SIL calculations developed in other software or tools and convert them into exSILentia. The exSILentia approach requires early engagement during the conceptual design.

> "The exSILentia approach for DeltaV SIS configuration leverages the SIL calculations and SRS captured in exSILentia, as well as the parallel structures between exSILentia and DeltaV SIS modules."

The use of the DeltaV SIS Configurator is mainly targeted to ESD applications. It is estimated that the tool could create up to 90 percent of the safety logic, depending on the complexity of the application. Currently there is no support for a sequential type of safety logic (e.g., BMS). Applicability to fire and gas is greatly affected by the lack of SIL calculations in these applications.

The exSILentia tool focuses on the generation of tag-based safety logic. The I/O configuration, including CHARM Smart Logic Solver (CSLS) configuration, CHARM configuration, and device allocation, is not part of the scope of the tool. With the DeltaV SIS late binding capability, the user can easily bind the tag-based configuration with the I/O design developed independently from SIF design. DeltaV Smart Commissioning is supported by configuration safety logic created by exSILentia. Graphics are not automatically generated either. Only a few alarms are configured by the tool; most SIS alarms must be configured manually or generated from alarm rationalization software.

Overview of exSILentia

The exSILentia product is an integrated suite of engineering software tools designed to support the process safety management (PSM) work process and the SIS functional safety life cycle. Data is seamlessly exchanged between the different phases of the safety life cycle, ensuring efficiency and consistency. Information from the process hazards analysis, layer of protection analysis, and SIL target selection are fed directly into the SRS. Once the SIFs and associated risk reduction requirements are defined, exSILentia SILVer facilitates the calculation of the achieved risk reduction for each SIF. Then, exSILentia enables the creation of an SRS that incorporates all the analysis done in the risk assessment.

The IEC 61511 standard requires the creation of an SRS and defines what the SRS should contain; exSILentia facilitates the compliance to IEC 61511 requirements. A proper SRS must contain all the requirements for the SIS and its associated SIFs. For each SIF, the SRS should include safe state, required SIL, maintenance and a startup overrides, architecture requirements, voting arrangements, trip delays, and other SIF requirements.

Emerson and exida collaboration

Emerson collaborated with exida to create a new approach for SIS configuration. By pairing built-in DeltaV SIS functionality with exida's comprehensive software tools, users can develop safety logic configurations much faster and in fewer steps.

In a traditional SIS configuration approach, the project team uses the SRS, along with a custom-built CEM as the basis for the safety logic configuration. The SRS and CEM are manually interpreted and translated into the safety logic. This configuration model requires multiple data entry stages and presents opportunities for human error. The new configuration approach powered by exSILentia leverages data structures created during the conceptual design to automatically generate safety logic (figure 5).

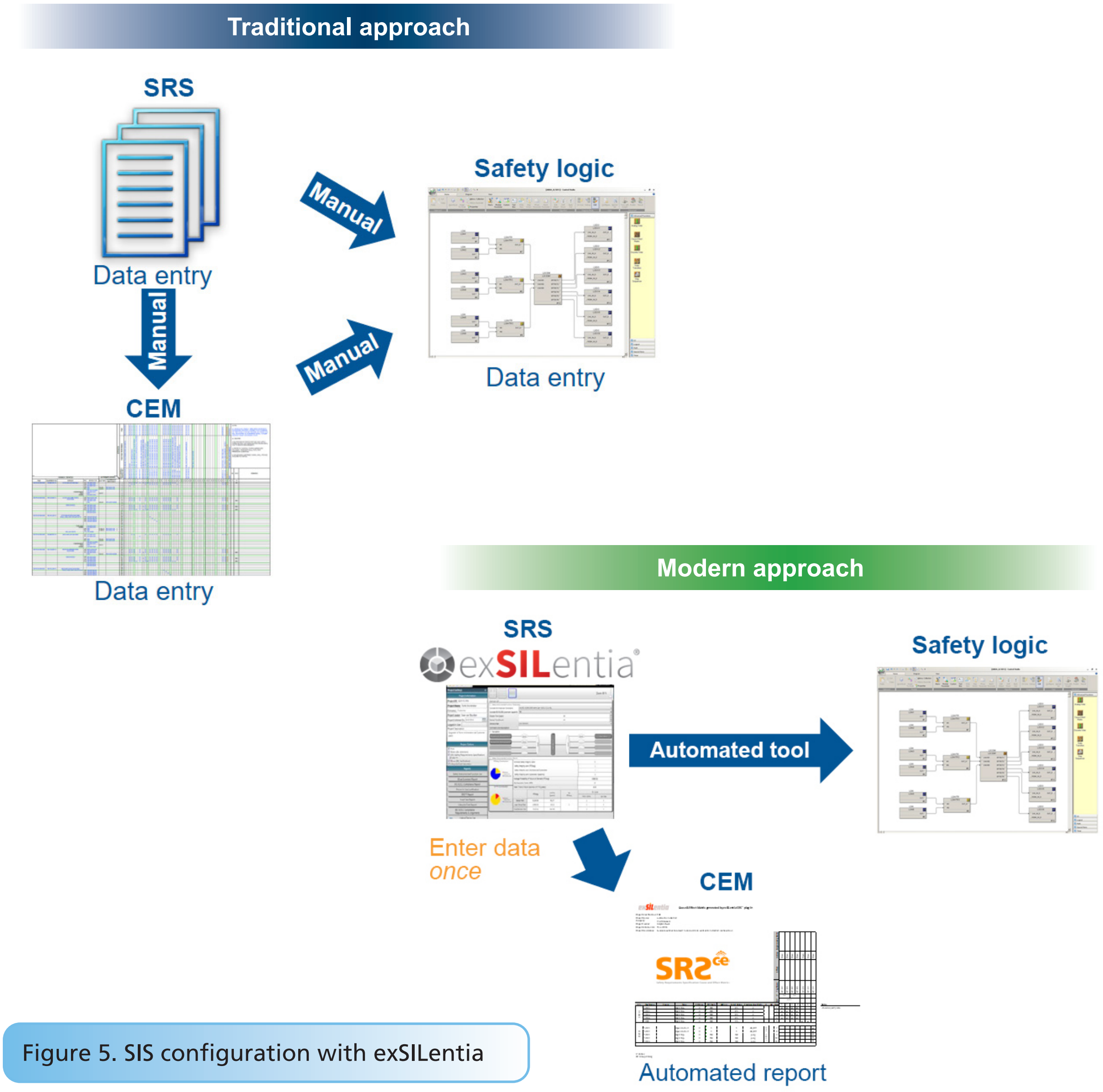


Figure 5. SIS configuration with exSILentia

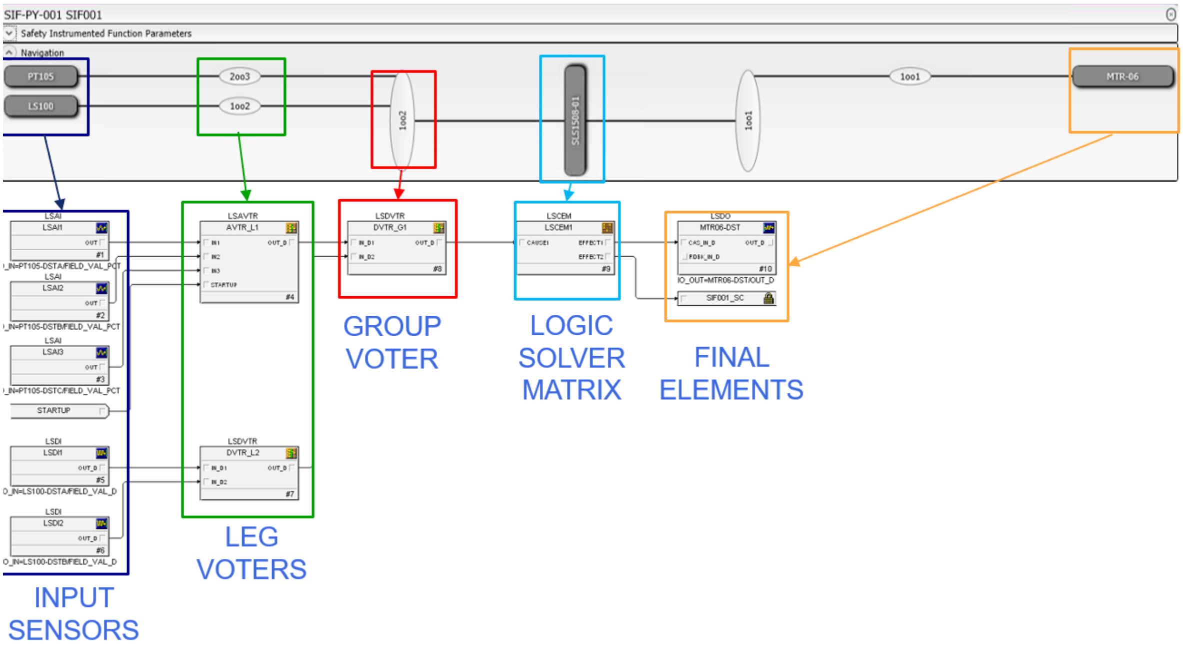


Figure 6. Parallel structures between exida and DeltaV SIS

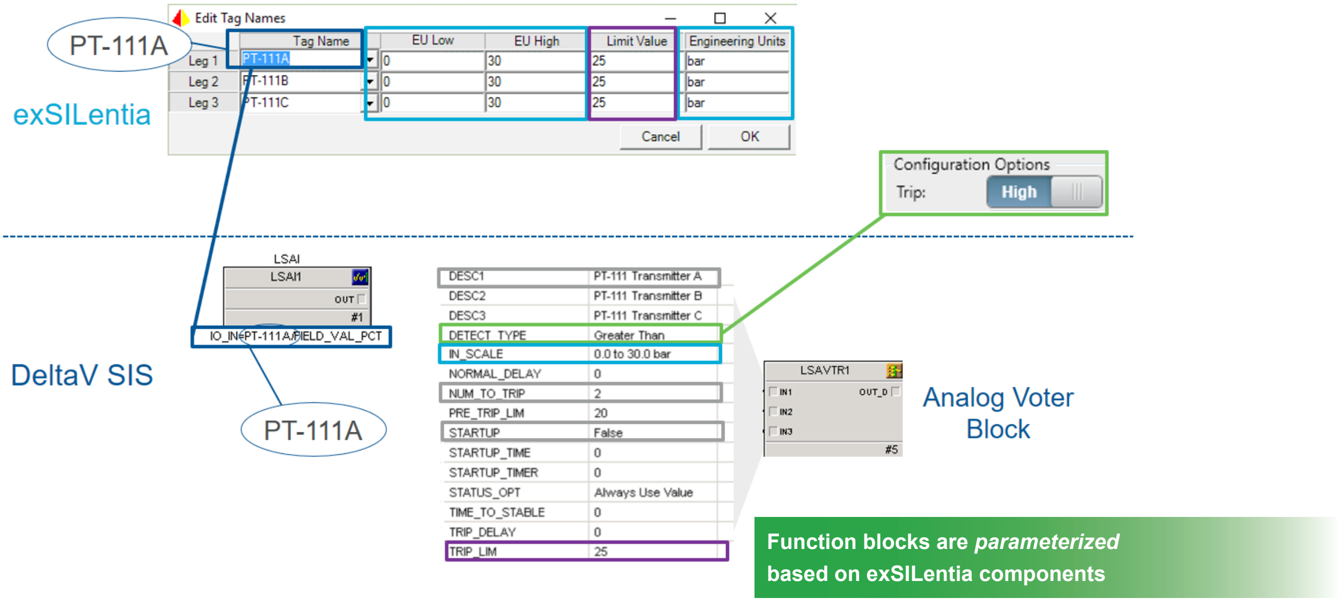
DeltaV SIS configuration using exSILentia

The DeltaV SIS Configurator created by exSILentia converts the exSILentia data into a DeltaV SIS configuration file (FHX file) that can be imported to create safety logic. The exSILentia approach for DeltaV SIS configuration uses the SIL calculations and SRS captured in exSILentia, as well as the parallel structures between exSILentia and DeltaV SIS modules (figure 6). Both exSILentia and DeltaV SIS follow an SIF approach that enables the overall SIS configuration to be divided into modular elements where a DeltaV SIS module contains one or more SIFs.

Each SIF contains a combination of sensors, voting arrangements, logic solvers, and final elements. Those elements defined in exSILentia are mapped to DeltaV SIS function blocks.

Creating SIS modules from exSILentia

The exSILentia solution defines DeltaV SIS function blocks and the appropriate connections based on the SIL calculation diagram (in SILVer). exSILentia also parameterizes the DeltaV SIS function



	Tag Name	EU Low	EU High	Limit Value	Engineering Units
Leg 1	PT-111A	0	30	25	bar
Leg 2	PT-111B	0	30	25	bar
Leg 3	PT-111C	0	30	25	bar

Configuration Options
Trip: High

IO_IN=PT-111A/FIELD_VAL_PCT

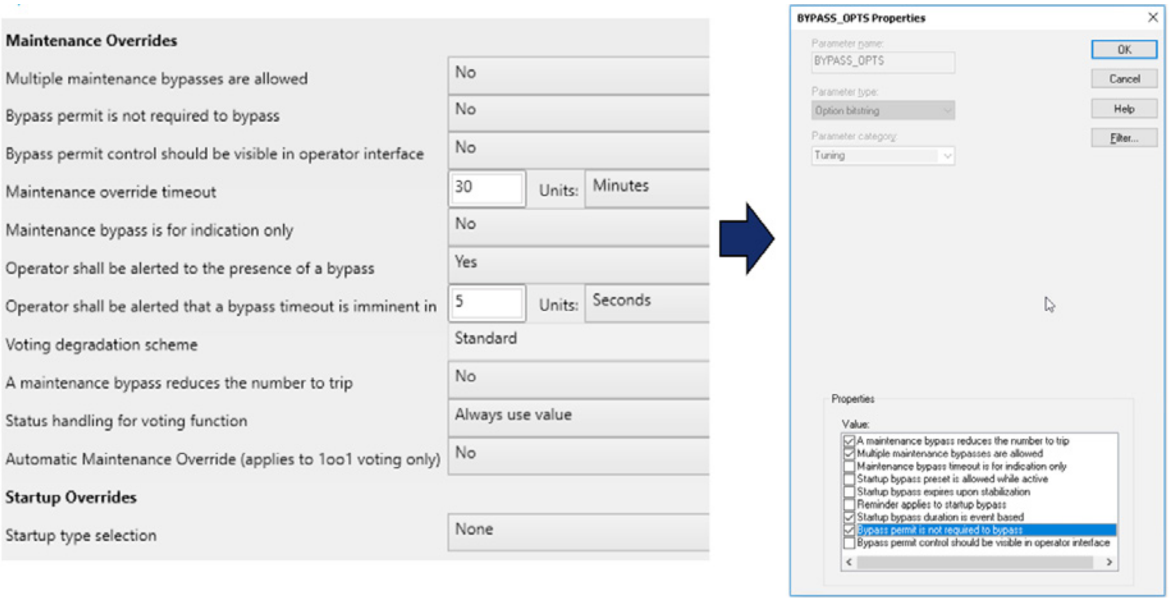
DESC1	PT-111 Transmitter A
DESC2	PT-111 Transmitter B
DESC3	PT-111 Transmitter C
DETECT_TYPE	Greater Than
IN_SCALE	0.0 to 30.0 bar
NORMAL_DELAY	0
NUM_TO_TRIP	2
PRE_TRIP_LIM	20
STARTUP	False
STARTUP_TIME	0
STARTUP_TIMER	0
STATUS_OPT	Always Use Value
TIME_TO_STABLE	0
TRIP_DELAY	0
TRIP_LIM	25

Function blocks are *parameterized* based on exSILentia components

Figure 7. Function block parameterization

blocks based on the exSILentia data. Parameters such as I/O tag, trip limits, ranges, engineering units, and trip direction are defined as part of SIF definitions within exSILentia. All those exSILentia settings are properly mapped to parameters within the DeltaV SIS function block (figure 7).

There also are parallel structures for maintenance overrides. The maintenance override requirements in exSILentia are mapped to the DeltaV SIS bypass option parameter (figure 8).



Maintenance Overrides	
Multiple maintenance bypasses are allowed	No
Bypass permit is not required to bypass	No
Bypass permit control should be visible in operator interface	No
Maintenance override timeout	30 Units: Minutes
Maintenance bypass is for indication only	No
Operator shall be alerted to the presence of a bypass	Yes
Operator shall be alerted that a bypass timeout is imminent in	5 Units: Seconds
Voting degradation scheme	Standard
A maintenance bypass reduces the number to trip	No
Status handling for voting function	Always use value
Automatic Maintenance Override (applies to 1oo1 voting only)	No
Startup Overrides	
Startup type selection	None

BYPASS_OPTS Properties

Parameter name: BYPASS_OPTS
Parameter type: Option bitstring
Parameter category: Tuning

Properties
Value:

☑ A maintenance bypass reduces the number to trip
☑ Multiple maintenance bypasses are allowed
☐ Maintenance bypass timeout is for indication only
☐ Startup bypass preset is allowed while active
☐ Startup bypass expires upon stabilization
☐ Reminder applies to startup bypass
☑ Startup bypass duration is event based
☑ Bypass permit is not required to bypass
☐ Bypass permit control should be visible in operator interface

Figure 8. Maintenance override in exSILentia and DeltaV SIS

SIFs sharing final elements are automatically combined into the same DeltaV SIS module, but users can also manually group SIFs into DeltaV SIS modules, even if those SIFs are not sharing a final element (figure 9).

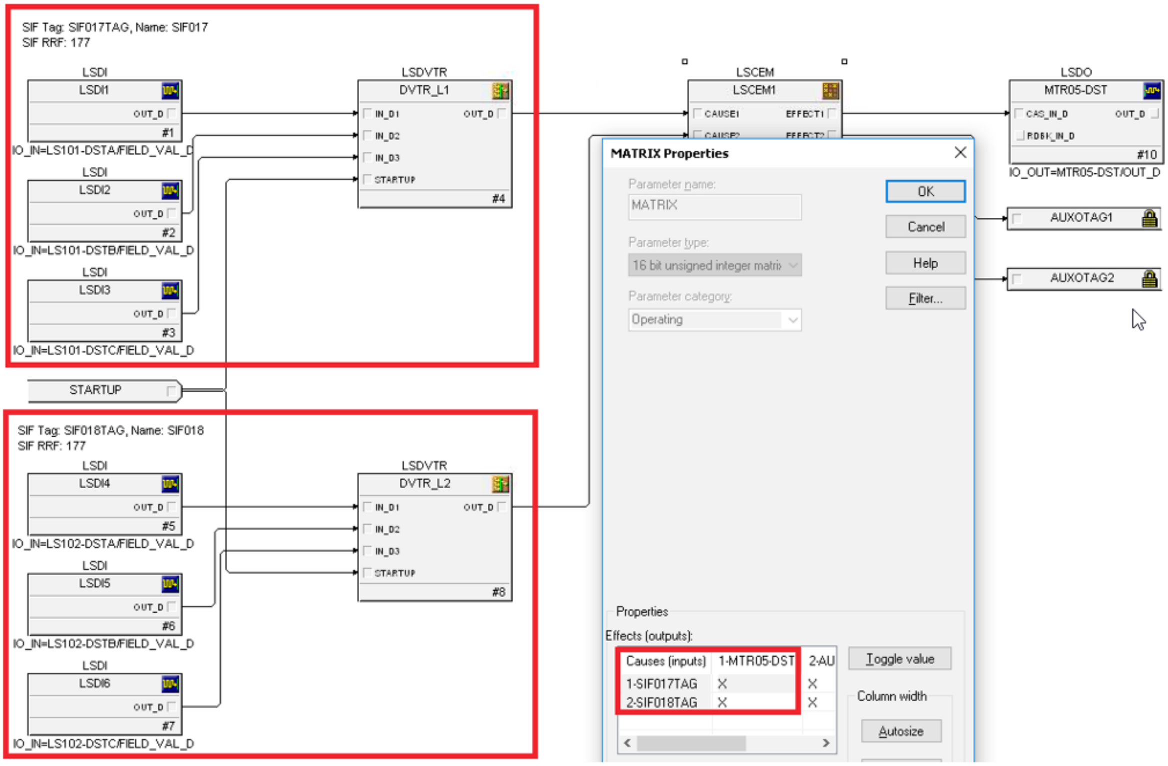
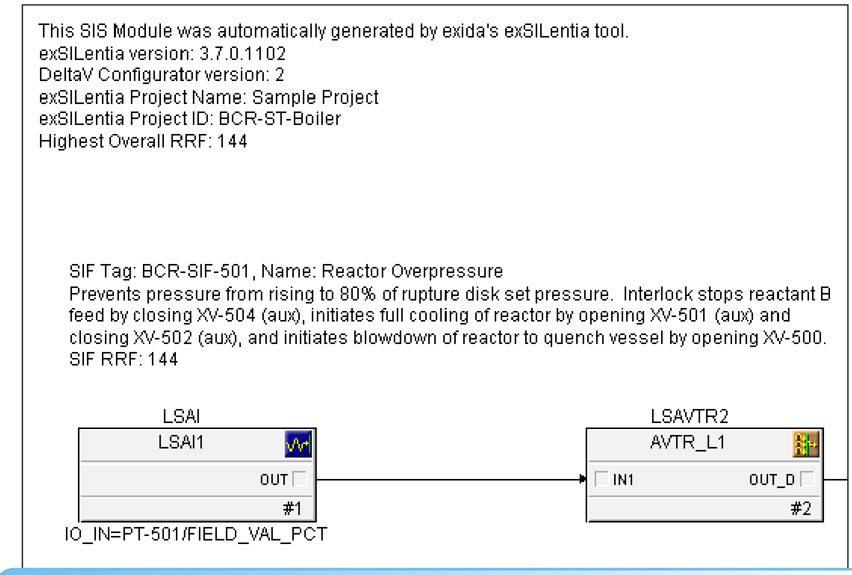


Figure 9. Automatically grouping of SIFs based on final elements

Annotations within SIS modules

One key feature is related to the ability to add proper annotations within the safety logic. exSILentia automatically adds relevant information that facilitates traceability to the SRS and increases logic readability (figure 10).


This SIS Module was automatically generated by exida's exSILentia tool.
exSILentia version: 3.7.0.1102
DeltaV Configurator version: 2
exSILentia Project Name: Sample Project
exSILentia Project ID: BCR-ST-Boiler
Highest Overall RRF: 144

SIF Tag: BCR-SIF-501, Name: Reactor Overpressure
Prevents pressure from rising to 80% of rupture disk set pressure. Interlock stops reactant B feed by closing XV-504 (aux), initiates full cooling of reactor by opening XV-501 (aux) and closing XV-502 (aux), and initiates blowdown of reactor to quench vessel by opening XV-500.
SIF RRF: 144

Figure 10. Annotation within DeltaV SIS modules created by exSILentia

Once the SIF definition and the design SRS are completed, the DeltaV SIS configuration can be generated using the SRS C&E menu in exSILentia (figure 11).

The user can choose to either generate the configuration for all SIFs or only selected SIFs (figure 12). The option for selected SIFs is useful for updating a SIF after late changes in the conceptual design.

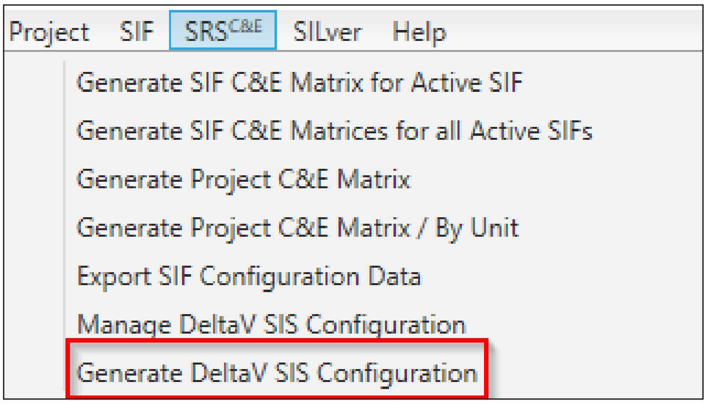
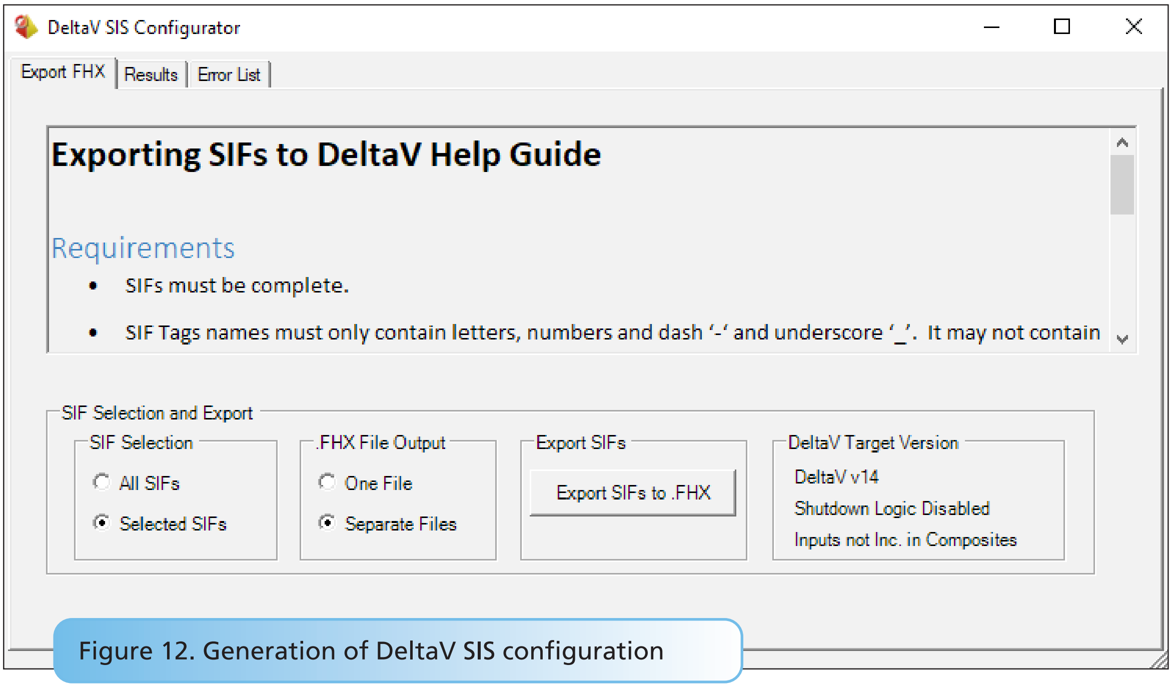


Figure 11. Generation of DeltaV SIS configuration



Exporting SIFs to DeltaV Help Guide

Requirements

- SIFs must be complete.
- SIF Tags names must only contain letters, numbers and dash '-' and underscore '_'. It may not contain

SIF Selection and Export

SIF Selection: ○ All SIFs ● Selected SIFs

.FHX File Output: ○ One File ● Separate Files

DeltaV Target Version
DeltaV v14
Shutdown Logic Disabled
Inputs not Inc. in Composites

Figure 12. Generation of DeltaV SIS configuration

Workflow for using exSILentia to generate DeltaV configuration

For end users and system integrators who already use or are intending to use the exSILentia tool, the DeltaV SIS Configurator plug-in allows them to automatically generate safety logic to be imported into the DeltaV SIS database.

The use of exSILentia within a DeltaV SIS project is described by the following short list of activities:

- **SIF modeling**. Once the SIFs are deemed required per the analysis phase, the SIF architecture is defined to meet the SIL requirement. exSILentia is used to specify and model the SIFs.
- **SIF detailing**. After the SIF architecture is defined, the user needs to detail the SIF within exSILentia. At this point, the user sets variable ranges, trip limits, etc.

- **Data transfer**. The exSILentia configuration file is now sent to the project team performing the DeltaV SIS configuration. In this approach, the exSILentia configuration file replaces the cause-and-effect diagram and other information typically sent to project teams.
- **SIF detailing for DeltaV SIS**. The project team will load the exSILentia database and will work on design details that the end user or system integrator does not necessarily need to care about during the analysis phase but are important for the configuration. This includes, for example, logic solver names associated with each SIF and sdefining the grouping of multiple SIFs into one single SIS module. The information is limited to safety logic and excludes graphics and I/O configuration beyond I/O references within I/O function blocks.
- **Configuration generation**. The project team will use exSILentia DeltaV Configurator to generate DeltaV SIS Logic (FHX files).
- **DeltaV import**. The project team will import the generated FHX file and finalize the DeltaV configuration not supported by exSILentia (i.e., alarms, I/O allocation and I/O binding, auxiliary actions implemented in BPCS, CHARM configuration).
- **Finalizing DeltaV configuration**. The project team will configure human-machine interface (HMI) graphics and verify logic implementation together with the HMI.
- **SIF logic validation**. The user will validate the SIF logic to verify proper connections and safety functionality for each SIF.

ABOUT THE AUTHOR

Serio Diaz is DeltaV SIS Product Marketing Manager at Emerson Automation Solutions. Find out more at www.emerson.com/deltav.

Related Articles

Understanding Fire and Gas Systems Increases Safety

Selecting the Best Control System for Automation Applications

Emerson Wins 2020 Exida Safety Award

IT/OT Convergence Delivers a Growing Range of Benefits

Continued Evolution for Process Automation

Alarm Management Solutions Continue to Outpace the Process Automation Market