Never waste a shutdown to improve process safety and uptime

Process safety cannot be ensured solely by design, as it relies on the effective operability of safety and control components. Effective operability is influenced by factors that include the condition of components and operational practices. Safety incidents with serious consequences can occur, even in well-designed facilities, if key components are not in proper operating condition, or if they are systematically bypassed.

Process safety is particularly important for potentially hazardous processes where abnormal conditions must be safely handled to protect assets, personnel, and environment. Moreover, increased regulations are pushing companies to validate, document, and prove process safety in a more continuous and systematic manner, as well as requiring auditable records for post-incident analysis and reports to authorities. Continuous process safety requires a proactive approach, leveraged by real-time analysis for promptly identifying areas of attention.

Two key components to process safety are safety instrumented systems (SISs) for performing safe shutdowns, and final elements that actuate on the processes. Both are designed and specified to achieve a nominal risk reduction that depends on their effective operability and activation rates.

For example, if final elements (such as safety valves) are stuck, or if frequent bypasses are activated by operators for too long, these conditions can compromise the timely execution of actions required for safe shutdowns. They can also increase the risk of catastrophic events. Additionally, if the demand rate on safety instrumented functions is higher than the nominal design limit, then the assumptions made for the probability of failure and required integrity level will not withstand. This further increases risk. These two examples demonstrate the need of a continuous analysis for effectively ensuring process safety, which requires validation of the components against the expected behaviors and limits.

Technical standards, such as IEC61511 and IEC 61508, provide guidance on the required validation activities of SISs as part of an overall safety lifecycle. However, these standards are not prescriptive on how to accomplish such validation. The typical approach for validation is through planned shutdowns and testing that require heavy data acquisition and processing. This approach is discontinuous, effort-intensive and prone to error.

Not a trivial task. The validation of SIS and final elements requires the analysis of a combined data set that includes alarms, events and process data. In this respect, hydrocarbon processing facilities can record hundreds of daily alarms and events reflecting safety and control operations, alarm status changes and control bypasses across all areas in a facility.

Validation is complex due to the need to collect, combine and analyze this vast amount of information in the proper context. This process must be accomplished in a structured way to understand what has happened (e.g., after a shutdown), considering the state of elements before and after a trip, process variables and control bypasses. The resulting sequence of events recorded must be considered to analyze how the actual behavior differed from expectations.

Collecting and analyzing data on spreadsheets or by using semi-automated tools is viable, but it is time-consuming and effort intensive. This method also requires a trained expert that might not be available onsite when needed to collect and analyze all the required data, as well as pinpoint issues and root causes. This validation is not a trivial task and must be completed as swiftly as possible to minimize downtime, which is a considerable collateral cost of validation. A thorough analysis must be carried out to identify root causes, particularly when unplanned shutdowns occur, before operations can be safely restarted.

All necessary reports must be generated to capture the outcome of the validation analysis, along with supporting data and comments for post-event analysis and auditing. This information should be made available to all intended stakeholders.

Considering the burden, complexity and costs involved for manual analysis, most companies schedule this only once or twice per year. While this can provide some insights, it may be too infrequent to keep pace with changing factors influencing process safety.

A new approach for real-time insights. An improved and proactive approach must leverage on advanced software capable of processing the continuous stream of data and events from facility control and safety operations, both planned and unplanned. This alternative approach combines the functions of automating and facilitating the validation, analysis and reporting on the condition of safety instrumented systems, as well as final control elements in a more continuous, structured and efficient way. These goals are accomplished by comparing against the expected behavior, and keeping supporting data for post-shutdown analysis, auditing and reporting to internal and external parties in the required format.

This advanced validation approach considers and flags any control bypasses that might have prevented expected actions that can be used to identify corrective actions required on operational practices. It enables remote collaboration for the analysis of all recorded safety operations, including the ability...
As the result of implementing an automated validation approach, the company facilitated collaboration between onsite personnel and remote subject matter experts. This customer was able to replace manual work previously accomplished by eight people who were semi-manually tracking and validating SISs, and redirect these resources to other value-adding activities. The customer is also able to complete a full shutdown validation 4–5 times faster than the previous manual validation method. This approach provided better confidence to restart securely, comply with IEC 61508/61511 and account for the required auditing reports mandated by regulating bodies.

**Benefits and takeaways.** This continuous and proactive approach automates, facilitates and improves the process of validating, analyzing and reporting on the operation of SISs and final elements. Benefits include:

- Faster validation of planned shutdowns, minimizing downtime and automatically generating supporting reports
- Early identification of issues for planning corrective measures, and increased production regularity
- Quick identification of root causes on unplanned shutdowns, and the application of correctives to restart operations faster
- Efficient validation and reporting on the operation of SISs and final elements, redirecting resources to other value-adding activities
- Remote collaboration and simplified workflow for validation, providing information to various required stakeholders, anytime and anywhere
- Consistency of conclusions, as the analysis does not rely on manual data processing or a single individual’s observation capability
- Fewer people required onsite for validation, lower travel costs and less exposure to risks
- Increased safety through continuous awareness of process safety
- Clear visibility into how bypasses could compromise safety, and ensured proper operational practices
- IEC615108/IEC61511 compliance
- Negotiation of lower insurance premiums is a possibility by showing a solution for systematic validation, auditing and reporting.

To improve process safety and uptime, begin leveraging data from planned and unplanned operations and never waste a shutdown again.

**Success stories.** This advanced process safety validation approach has been utilized by many companies ([FIG. 1](#)). One success story is a company running sites in harsh locations and under stringent process safety regulations. The company sought a more efficient and effective solution for validating the condition of thousands of safety instrumented functions (SIFs), the ability to more closely examine actual demand rates on SIFs, and the minimization of the downtime required to perform any validation—either planned for compliance with regulating agencies or unplanned shutdowns—to quickly identify root causes and actions required for a fast and safe restart.

**FIG. 1.** With advanced applications, companies can exploit unplanned shutdown data to improve safety and uptime.

![FIG. 1. With advanced applications, companies can exploit unplanned shutdown data to improve safety and uptime.](image)


---

**MICHELE LOSETO** is a Product Manager at Honeywell Process Solutions. He has more than 18 years of experience developing and implementing oil & gas solutions aimed to improve remote monitoring, performance and safety. He is an MBA and holds a degree in electronic engineering. E-mail him at michele.loseto@honeywell.com.

To learn more about Honeywell’s Process Safety Analyzer, please visit [http://hwll.co/psa](http://hwll.co/psa).