Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation

API BULLETIN 16H
FIRST EDITION, XXXX 202X

Table of Contents

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed. Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict. API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

The verbal forms used to express the provisions in this document are as follows.

— Shall: As used in a standard, “shall” denotes a minimum requirement to conform to the standard.

— Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required to conform to the standard.

— May: As used in a standard, “may” denotes a course of action permissible within the limits of a standard.

— Can: As used in a standard, “can” denotes a statement of possibility or capability.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001.

Suggested revisions are invited and should be submitted to the Standards Department, API, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001, standards@api.org.

Introduction

This bulletin provides information on the best available and safest technologies that could be integrated to bring a well to a safe state in the event other operational barriers fail. This publication is under the jurisdiction of the API Committee on Standardization of Oilfield Equipment and Materials (CSOEM).

This bulletin discusses the strategies to create an automated blowout preventer actuation system, the challenges and obstacles associated with this type of system, current existing technology, and the methods of achieving widespread implementation of such a system.

An automated safety instrumented system is intended to bring the well to a safe state in the event that the site personnel do not recognize a well influx or are unable to respond to one. Safety instrumented systems have been utilized in process (e.g., refineries, chemical, nuclear) facilities as an integral part of a critical process system.

The implementation of an automated safety instrumented system should consist of input from the lease operator, drilling contractor, and original equipment manufacturer.

1 Scope

1.1 This bulletin provides a review of the equipment and interfaces to be considered for the automation of a blowout preventer to place the well in a safe state in an onshore environment.

1.2 This bulletin provides an overview of components that can be considered for future research into developing an automated well control actuation system such as:

a) top drive and kelly drive;

b) hook load weight indicators;

c) drawworks;

d) mud pumps;

e) blowout preventers (BOPs);

f) BOP control system (closing unit);

g) Internal BOP and/or full-opening safety valve;

h) choke manifold;

i) programmable logic controller;

j) pressure control valve (pilot valve);

k) surface and downhole blowout preventer;

l) pipe tallies;

m) managed pressure drilling equipment;

n) open and closed channel flow meters;

o) and pit level sensors.

1.3 To the extent that this document reviews specific equipment arrangements, it is recognized that other arrangements can be equally evaluated in addressing well requirements and achieving safety and operational efficiency.

2 Normative References

The following referenced document is indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

There are no normative references in this document.

3 Terms, Definitions, and Abbreviations

3.1 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
black channel
A communication channel with unsecured properties or properties that do not fit the application

3.1.2
blowout preventer
BOP
Equipment installed on the wellhead or wellhead assemblies to contain wellbore fluids either in the annular space between the casing and the tubulars, or in an open hole during well drilling, completion, and testing operations.

3.1.3
blowout preventer control system
closing unit
The assembly of pumps, valves, lines, accumulators, and other items necessary to open and close the blowout preventer equipment.

3.1.4
bottom-up integration testing
Testing the lowest units of the application and gradually moving up one-by-one

3.1.5
remote control station/panel
A panel containing a series of controls that will operate the BOP functions from a location that is remote from the hydraulic control manifold or central processor in the case of a multiplex control system (MUX).

3.1.6
drilling control system
DCS
A controlling system for mechanical equipment with display and storage of drilling data, alarm handling, and process control.

3.1.7
equipment under control
EUC
The set of all equipment, machinery, apparatus or facility that gives rise to hazardous events for which the safety-related system is required.

3.1.8
false negative
A test result that incorrectly indicates that an event is absent when one occurs.

3.1.9
false positive
A test result that incorrectly indicates that an event is present when one does not occur.

3.1.10
instrumented protective system
A safety system composed of a separate and independent combination of sensors, logic solvers, final elements, and support systems that are designed and managed to achieve a specified risk reduction.

3.1.11
kelly drive
A type of well drilling device on a drilling rig that employs a section of pipe with a polygonal (three-, four-, six-, or eight-sided) or splined outer surface, which passes through the matching polygonal or splined kelly (mating) bushing and rotary table.

3.1.12
kick
Intrusion of formation fluids into the wellbore.

3.1.13
pipe tally
The current total number of drill pipes (including the bottom-hole assembly) in use.

3.1.14
programmable logic controller
PLC
A microprocessor-based device capable of controlling many types of industrial equipment and entire automated systems.

3.1.15
programmable logic relays
PLR
Hard wired control system using instrumentation, switches, timers, relays, contactors, motors, and actuators.

3.1.16
remote telemetry unit
RTU
A microprocessor-based devise connected to sensors, transmitters, or process equipment for the purpose of remote control.

3.1.17
remote terminal unit
A multipurpose device used for remote monitoring and control of various devices and systems for automation.

3.1.18
safe state
The state of the process after acting to mitigate the hazard.

3.1.19
safety instrumented system
A system composed of sensors, a logic solver, and final control elements for taking the process to a safe state when a predetermined process condition is exceeded.

3.1.20
sandwich integration testing
The combination of the top-down and bottom-up approach by testing on the layer from the top to the middle layer and on the layer from the bottom to middle.

3.1.21
supervisory control and data acquisition
A computer-based monitoring and control system that collects, displays, and stores information from remotely located data collection units and sensors to support the control of equipment, devices, and facilities.

3.1.22
top-down integration testing
Testing the top-most modules and gradually moving down to the lowest set of modules one-by-one

3.1.23
top drive
A device that can be hoisted in the derrick or mast of a drilling rig that rotates the drillstring

3.1.24
well control system
The equipment, assemblies, subassemblies and subsystems integrated to prevent the uncontrolled release of high-pressure fluids (oil, gas, or salt water) from subsurface formations.

3.2 Abbreviations

ALARP	as low as reasonably practicable
ALARA	as low as reasonably achievable
BHA	bottom-hole assembly
BHP	bottom-hole pressure
BOP	blowout preventer
DCS	drilling control system
ECD	equivalent circulating density
EDR	electronic drilling recorders
HMI	human machine interface
IPS	instrumented protective system
MPD	managed pressure drilling
OEM	original equipment manufacturer
PLC	programmable / process logic controller
PLR	programmable logic relay
PVT	pit volme totalizer
RCD	rotating control device
RTU	remote telemetry unit

SIS	safety instrumented system
SCADA	supervisory control and data acquisition
WCS	well control system

4 Key Elements of Automated Safety Instrumented Systems

4.1 General

The following sections identify key elements to consider when designing, testing, and implementing a system that can automate the process of bringing a well to a safe state by shutting in the BOP.

4.2 Objective

The monitoring equipment, logic solver types, equipment under control, and operational controls listed below, should be individually assessed to determine the applicability into an Safety Instrumented System (SIS). Original Equipment Manufacturers (OEM), lease operators, and drilling contractors should work together to evaluate the individual and combined components of an SIS.

4.3 Description

4.3.1 Monitoring Equipment

4.3.1.1 Hook Load Weight Indicators

These devices are used to display the weight being supported by the hook. This can include the drill string, drill collars, bottom-hole assembly (BHA), casing, bit, and any other component in the load path below the hook. These weight indicators can be analog or digital. A calibrated load cell is typically connected to deadline side and a calculated value that accounts for any losses, such as sheave friction, is displayed. Most indicators have a tare function that allows the driller to set a zero-reference point for precise load measurements.

4.3.1.2 Managed Pressure Drilling Equipment

Managed pressure drilling (MPD) equipment is used to precisely control the annular pressure profile in the wellbore. MPD comes in many forms such as dual gradient drilling (DGD), applied surface backpressure, controlled mud level (CML), pressurized mud cap drilling (PMCD), and floating mud cap drilling (FMCD) to name a few. The applied surface backpressure method is the most common in use and is described here. This method typically consists of equipment such as a rotating control device (RCD), drill string isolation tool (DSIT), flow spool, buffer manifold, buffer tank, metering manifold, and MPD choke manifold, depending on the application .

The idea with this method is to use a light annular mud weight in combination with an applied surface back pressure to keep a constant bottom-hole pressure (BHP). This allows drilling through formations with tight drilling windows, thief zones, etc. where conventional drilling can be problematic.

4.3.1.3 Open and Closed Channel Flow Meters

These devices provide the rate of fluid flow in an open or closed flowline. These can be of various types such as flow-paddle, flow-wheel, turbine, or ultrasonic.

4.3.1.4 Pit Level Sensors

These devices provide a level of the drilling mud contained in the rig’s mud pits. They are typically either the ultrasonic or float types. The ultrasonic type uses ultrasonic wave refraction to measure the vertical distance from the sensor to the top surface of the mud. The float type uses a float element and electrical resistance to provide a similar measurement.

Knowing accurate pit levels can help identify potentially unstable well conditions, such as influxes or losses. This information is critical for an automated SIS.

4.3.1.5 Pipe Tallies

4.3.1.5.1 Pipe tallies are used in conjunction with the length to help the driller know the exact location of the drill bit or other drill string component datum. They can be manual or automated tallies.

4.3.1.5.2 Automated tallies typically use some type of technology to uniquely identify each drill pipe such as an radio frequency identification (RFID) tag or similar device. Other methods such as drill pipe telemetry or a database of drill pipe particulars may be used.

4.3.1.5.3 Automated or manual pipe tallies are used in an automated SIS to communicate essential drill string information (i.e., tool joint location) in the event that spacing out is required prior to bringing the well to a safe state. If manual pipe tallies are used, the information would require digitalization. Both require an interface to the drilling control system (DCS). Other technologies may be capable of identifying tool joints within the well bore.

4.3.2 Logic Solver

4.3.2.1 Supervisory Control and Data Acquisition

Supervisory control and data acquisition (SCADA) utilize programmable logic controllers (PLCs), remote terminal units, or similar technologies. These microprocessor-based systems collects information about a well control system with the capability to control the shut-in operation.

4.3.2.2 Programmable Logic Controller

PLCs can provide automation sequencing and industrial process control and are used in a variety of industries. All of the associated components and functions are centered on the controller. The controller is programmed based on predetermined parameters to perform a specific task. Once programmed, these systems can perform many functions, providing a variety of analog and digital input and output interfaces; signal processing; data conversion; and various communication protocols.

4.3.2.3 Programmable Logic Relays

Programmable logic relays are similar in functionality to PLCs, although they have limited scalability.

4.3.2.4 Remote Telemetry Units

A remote telemetry unit (RTU) transmits bidirectional data from sensors located on mechanical components and monitoring equipment and transmitted to equipment under control. The data from RTUs are either at defined intervals or by exception. Control algorithms can be established to provide on/off control or a variable control.

4.3.3 Equipment Under Control

4.3.3.1 Drilling Control System

The DCS is the main interface for the driller to operate the drilling equipment. These systems can be fully integrated with all mechanical components or be comprised of individual systems that are controlled in a central location (i.e., driller's control room). This system controls all the equipment needed to drill the well. This system is comprised of the following equipment:

4.3.3.1.1 Top Drive and Kelly Drive

The top drive is a device suspended in the derrick that during drilling operations serves the following functions: rotating the drillstring, providing a conduit for drilling mud, disconnecting/connecting pipe, closing in the drill pipe by an integrated kelly valve, and lifting/lowering the drill string by use of the elevator. Top drives can be electrically or hydraulically driven.

4.3.3.1.2 Drawworks

Drawworks are hoisting mechanisms, or winch, used to spool the hoisting cable in a controlled fashion.

4.3.3.1.3 Subsurface Safety Valves

Subsurface safety valves are devices used to isolate wellbore pressure and fluids. They are traditionally fail-safe closed requiring a signal to remain open.

4.3.3.1.4 Mud Pumps

Mud pumps are utilized to circulate drilling fluid in the well. The fluid, usually drilling mud, is pumped down the drill string and returns to surface through the annulus of the wellbore.

4.3.3.2 Well Control System

The well control system (WCS) is used to bring the well to a safe state after the detection of an influx and may be considered as a Basic Process Control System (BPCS). Human-machine intervention is currently required to facilitate the functionality of the WCS. This equipment is generally classified as pressure control equipment and is distinctively different than other equipment that is unable to contain wellbore pressure such as the HP mud system. This system is comprised of the equipment described in the following sections.

4.3.3.2.1 Blowout Preventer

Blowout preventers (BOP), whether annular or ram type, are equipment installed on the wellhead for the express purpose of containing wellbore fluids in the annular space between the casing and tubulars or in an open hole during well drilling, completion, and testing operations. BOPs are available in a wide range of pressure ratings between 1,000 psi (6.9 MPa) and 30,000 psi (206.8 MPa) and bore sizes ranging from 7-1/16 in. to 30 in.

Ram-type BOPs utilize metal blocks with assembled elastomer seals, or rams, to seal off pressure on a wellbore. There are three main types of rams: blind, blind shear, and pipe. Blind rams are used to fully close and seal the wellbore when no tubulars are present in the bore. Blind shear rams are capable of sealing on an open hole and cutting various tubulars and cables that could be present during operation prior to engaging the wellbore seal. Pipe rams are utilized to seal between the annulus bore and the outside of tubulars that are in the bore. Pipe rams are available in either a fixed diameter, sealing on only a specified pipe size, or a variable diameter that is capable of sealing on a range of tubular sizes.

Annular BOPs utilize an elastomeric sealing element to seal the space between the tubular and the wellbore or an open hole. The ability to seal on a large range of tubular sizes is the primary advantage of the annular BOP, which is generally located at the top of a BOP Stack and may have a lower rated working pressure than the ram-type BOPs below. When annular BOP elements are closed on an open hole, the pressure rating is reduced to 50% of the rated working pressure of the BOP. Review pressure sensors inclusion in next meeting. Stopped here!!!!!

4.3.3.2.2 Choke Manifold

The choke manifold, sometimes referred to as a choke and kill manifold, is an assembly of valves, chokes, gauges, and lines used to control the rate of flow and pressure from the well when the BOPs are closed. The choke manifold may bleed off wellbore pressure at a controlled rate or may stop fluid flow from the wellbore completely. It is connected by means of a high-pressure pipe or hose to the BOP Stack either through a drilling spool or directly to the side outlet of a ram-type BOP.

4.3.3.2.3 Accumulator

Accumulators are pressure vessels charged with inert gas and used to store hydraulic fluid under pressure. The inert gas is maintained at a precharge level pressure such that when the hydraulic fluid is pumped into the accumulator, the gas is further compressed thereby storing potential energy utilized by the BOP control system to function the BOP Stack during operation. An assemblage of accumulators is referred to as an accumulator bank.

4.3.3.2.4 Pressure Control Valve

A control valve is a component in the BOP control system that directs power fluid to operate a selected function of the BOP stack. The control valve typically receives a hydraulic signal through the pilot line to operate the selected function.

4.3.3.2.5 BOP Control System

The BOP control system is a hydraulic or electrical assembly of pumps, valves, lines, accumulators, and other items necessary to open and close the well control equipment utilized in drilling and completions operations. These systems are remotely located from the BOP and can be direct hydraulic or electric-over hydraulic in operation. Control of individual operations may be through manual operation of a valve or through interaction with push-button or touchscreen interfaces.

4.3.4 Operational Barriers

4.3.4.1 Hydrostatic Pressure

Hydrostatic pressure occurs when a column of fluid imposes a force due to gravity. One purpose of this fluid is to control well pressures by opposing the natural formation pore pressure. The hydrostatic pressure is directly related to the density of the fluid. Movement of the fluid changes the hydraulic force applied with the fluid in use due to frictional forces.

4.3.4.2 Human Detection and Action

These aid in the effectiveness of a physical well control barrier. Based on observations, a specific plan or procedure can be followed to function a piece of equipment.

EXAMPLE Detection of an influx while drilling and the process to close BOPs, including steps to sound alarm, stop rotary, turn off pumps, space out string tool joint, and/or activate accumulator to close appropriate pipe ram.

4.3.4.3 Procedures

The lease operator and drilling contractor should agree on a predefined series of steps to be followed in a regular definite order to accomplish a task. Well control procedures should also be evaluated that could be used to properly aid in the effectiveness of a physical barrier. Additionally, equipment, interface, and operating parameters of the SIS should be discussed and agreed upon by the lease operator and drilling contractor prior to deploying an automated system capable of bringing the well to a safe state.

Procedures should consider the use of advanced technology such as kick detection systems and Artificial Intelligence (AI). Human interaction with these system should be clearly defined. A kick detection system can provide the first indication that a well is becoming unstable. The use of a kick detection system is required for automated actuation of the BOP system in the event rig personnel do not identify the influx and react. The alarm circuits or software, or both, should be designed so the frequency of false indication(s) is eliminated or reduced to a minimum level without compromising the ability of the system to provide indication of an abnormal condition to the equipment operators.

Artificial intelligence, specifically the application of machine learning should be considered when designing automated blowout prevention equipment and systems capable of bringing a well to a safe state from a kick.

5 Obstacles and Challenges

5.1 General

Emerging technologies such as those utilized to develop automated safety instrumented systems have the potential to transform and empower the oil and gas exploration community. These technologies can help expand, automate, and mitigate unexpected events resulting in a loss of primary well control. Major topics that create potential obstacles and challenges will be reviewed to aid in identifying limiters to advancements in integrating systems. This is not an all-inclusive list.

5.2 Description

SIS, if not integrated properly, can result in reduced operational efficiency, increased downtime, operational risk, and potential loss of assets.

5.2.1 Safety Requirements Specification / Functional Safety Management Plan

Prior to any development of an automated SIS, a functional safety life-cycle for the system should be established. Integral to the safety life-cycle is the development of the Safety Requirements Specification (SRS) and the Functional Safety Management Plan (FSMP). Both of those documents drive not only the HW and SW development of the system but the processes related to the entire lifecycle of the automated SIS.

The SRS is the key development document that drives the entire technical design of SIS. It establishes and identifies the Safety Instrumented Functions (SIFs) that make up the SIS. The document contains the necessary functional and performance requirements to achieve a safe state shutdown for each SIF. Each SIF is identified during the safety planning phase and should include the driller, OEM, customer and/or the certifying authority. A third-party moderator can also be included in the development of the SRS. In general, the end user should provide the functions that comprise the SIFs.

The FSMP is intended to establish the process guidelines that qualify and certify the SIS. The FSMP is used to describe the process and procedures used to design, verify, validate, and maintain the system. Contained within the FSMP should be the Clause 5 requirements of IEC 61511-1. Those include Quality Assurance, Risk Assessment planning, implementation, configuration management, SIS architecture, etc.

The FSMP should also specify the ownership of the different phases between the OEM and the final user. In general, the OEM owns this document. The Safety Life-Cycle phases, requirements, and steps are listed in IEC 61511-1 and ISA 84-1.

5.2.2 Integrating and Modifying Systems

5.2.2.1 Proprietary Software

Using propriety software to develop automated safety instrumented systems has numerous obstacles and challenges including cost, developer support, security issues, and customization. When compared to open source software, proprietary software cost can be exponentially increased due to licensing fees. Licensing fees can vary depending on the number of licenses obtained. Maintenance fees are often included in proprietary software costs.

The end user may be dependent on the program's developer for all updates, support, and fixes. Another drawback is that you cannot modify or customize the software. Development and delivery of updates to programs can vary depending on the size of the development team. Critical issues such as security holes and other problems may make the timely delivery of updates an important aspect of software support. Further challenges would be encountered if a primary developer goes out of business. No further updates or support would be available unless another company buys out the project.

Due to limited availability of source code to the public, security issues may not be fixed as rapidly as open-source software. The development team is the primary source for identifying problems and security loopholes.

When developing a safety instrumented system both open source and fully proprietary software have the disadvantage of no internationally recognized safety certification. This lack of certification can cause extended validation cycles that may be prohibitive and limit the development team's ability to provide quick turn customizations. Another possibility is to select a platform that has a safety certified limited variability language as defined in IEC 61508-3 and a failsafe communication methodology such as Black Channel. The SIS application can be built on top of these tools to facilitate certification of a safety integrity level.

Software customization would be the responsibility of the development team. Lease operator requirements or requests may create the need for frequent software customizations. Also, adaptability associated with constant change in the information technology field may create obstacles while the inaccessibility of the programs source code may create limiters to software customization.

5.2.2.2 Intellectual Property

Protecting intellectual property (IP) rights can be very costly. An automated safety instrumented system can be a very complex product that involves designs, methods, and processes. To protect the developer's intellectual property rights several patent applications to protect one's product may be required. Agreements on IP ownership between all parties should be established at the beginning of the project.

As intellectual property rights diminish, the quality of the product being created may also diminish. The incentive to dedicate time and resources to adequately develop software platforms could be reduced, especially if the company knows it attained its intellectual property rights fortuitously.

5.2.2.3 Working with Multiple OEMs

When multiple original equipment manufacturers are involved, a principal contractor should be selected. The principal may insist on design, method, or process changes not based on market requirements but influenced by internal perspectives. A lack of product understanding may require other manufactures to provide technical support unnecessarily exhausting time and resources. Improvements in automated safety system design and integration may be hampered due to exclusivity created by an original equipment manufacturer.

5.2.3 Kick Detection System

5.2.3.1 General

A kick detection system is a system designed to identify abnormal flow from the well based on sensor inputs. These complex, algorithmic systems target identification on smaller scales (and sooner) than rig personnel typically are able to identify. The system should be operation state-based, where different parameters and set-points can be utilized and incorporate machined learning capabilities. Additionally, kick detection systems help to reduce nuisance alarms that create alarm fatigue. Minimum and maximum parameters should be established to eliminate nuisance alarms ALARP or ALARA and to reduce potential alarm fatigue. The kick detection system can pose both false positive and false negative results within the instrumentation.

5.2.3.2 False Positives

Incorrectly alarming on an event that proves to be false. False positive indicators from systems negatively impact trust from humans and therefore reduce the effectiveness of the system. Too many false positives will encourage the system to be disabled to prevent reoccurrences. The system should be designed so false positives are kept to a minimum.

5.2.3.3 False Negatives

A false negative occurs when the system fails to identify inputs that indicate a well is unstable or that an event is occurring. False negative prevention is key to the systems reliability and effectiveness. If the system does not identify a kick, then the purpose of the system is lost. The risk of incurring a false negative should be reduced to as a low as reasonably practicable.

5.2.4 Cybersecurity

As with any computer-based system, security is a key element in system reliability. The criticality of a system increases the emphasis that cybersecurity should be designed around. The systems in this document are assisting a critical task of identifying flow or kick events and should be considered critical.

Obstacles and challenges may arise from the use of universal serial bus (USB) and remote access equipment. Potential methods of disruption or system failure can be sourced from external devices interacting with the DCS and WCS. The system allowing USB devices such as memory sticks, smart phones, and other devices should have additional security checks before allowing these devices to make changes to the system.

Allowing remote access via network or cellular connection may be useful for system updates and improvements but may also allow malicious changes to the system. Any external access to the system should be secured to prevent unauthorized system changes.

Standards are available to assess the cybersecurity capability of systems. The standards specify how to assess the threat landscape, do risk assessments, harden the system, execute penetration testing, etc. For more information see IEC 62443 and ISA 84. Use of these standards provides a robust, risk based method of assessing systems that need features like cloud connectivity.

5.2.5 Testing

5.2.5.1 Endurance and Performance Testing

Endurance and performance testing refers to tests performed to find out whether the system can withstand the processing load it is expected to endure for the period of the well and several wells. During endurance tests, the system is observed to determine potential failures. The system's performance quality should also be monitored during endurance testing. For safety instrumented systems performance testing should also include fault injection testing. This can require setting up specific failure conditions in the system under test and assuring the SIS reacts appropriately.

During development and prior to deployment the system should be tested with operational type loads. These loads would be extended over a significant amount of time creating a challenge relating to time constraints. The aim would be to evaluate the behavior and performance of the system during sustained use eliminating potential obstacles during deployment. This type of testing is performed to ensure challenges associated with premature failures to demonstrate the software and hardware integrations are capable of handling as well as interpreting the data without any deterioration in response time.

Endurance and performance tests should measure the system's response and response times under potential simulated conditions for a specific period and for a certain threshold. These observations should then be used to further enhance the system's parameters and reliability.

Endurance and performance tests should be performed for an extended period of time, simulating extended well drilling activities. The extended period of testing ensures the system can handle the hardware resource issues, such as a memory shortage, that could cause the system to crash or function improperly.

Endurance testing is performed after the establishment of the design, methods, processes, fabrication, and initial troubleshooting at the last stage of development prior to deployment to reveal actual or potential functionality limiters. Endurance testing can create challenges by requiring prolonged testing processes taking several years to achieve accurate system performance resulting in an extended period of time for deployment. Endurance testing creates time constraint challenges by simulating all aspects of a rig environment from rig move, to rig up, function testing in drilling type environments inclusive of a multitude of scenarios, and through rig down to ensure the robustness of the system. Inadequate endurance testing can result in obstacles secondary to the premature functioning of the automated safety instrumented system.

System hardening and penetration testing (IEC 62443 and ISA 84) should identify and eliminate cybersecurity issues. Endurance and performance testing should identify and eliminate false positives and false negatives from given scenarios encountered during well drilling activities.

5.2.5.2 Site Integration and User Acceptance Testing

Site integration testing is the overall testing of the whole integrated system, which is composed of the drilling control system, electronic drilling recorder (EDR) and pit volume totalizer (PVT) systems, the automated SIS, and any other sub-systems. The main objective of site integration testing is to ensure that all software module interactions and dependencies are communicating and functioning properly and data integrity is preserved between distinct modules of the whole system.

NOTE: Site integration testing refers to each time the system is disassembled and reassembled at a new location

The site integration testing should be performed to ensure the behavior of all systems coexist and function as expected once powered up, brought online, and integrated. SIS signals, diagnostics, bypasses, and alarms displayed on shared or individual human machine interface (HMI) screens should be tested during this stage.

The site integration test should be performed after the initial rig up and before spudding the well. This should also include testing the procedures for rigging and powering up the system. The deliverables of the site integration test should be defined, passed, and signed off as a part of the user acceptance test.

Various factors such as databases, platforms, environment, PLCs, DCS, and WCS, may create difficulties. These difficulties could be a result of a number of legacy equipment that require integration of automated safety instrumented system components. Integrating a new system to a legacy system would require a large amount of testing and modifications. Developers will also realize there will be less compatibility between the two systems developed by two different companies. There will also be numerous paths and variables to apply to adequately test the integrated systems creating necessary development hurdles.

Additional challenges include, incremental integration testing needs to connect two or more components together based on their logic profiles. After testing, additional modules would be added to aid in fault localization reducing potential obstacles and challenges. The process would continue until all modules have been integrated and successfully tested. The top-down, bottom-up, and sandwich integration testing approaches will create time and resource requirements to adequately commission an integrated system.

5.2.6 Human Factors

5.2.6.1 Acceptance of an Automated BOP

Inadequate information, demonstration, and training provided to the users could create an atmosphere of apprehension. This lack of core structure leads to scenarios the users cannot predict due to a lack of knowledge, skills, and experience with SISs. A diminished sense of control can be created potentially leading to the bypassing of automated systems because the systems reliability and functionality has not been widely accepted.

Crew training and involvement in the devlopment and testing of the SIS can help mitigate human factors associated with this resistance to change. Clear definition of roles and responsibilities for each user of the system should be established. Refer to section 5.2.6.4 for further information.

5.2.6.2 Audible and Visual Indicators

The selection, control, design, and arrangement of controls and displays will be an imperative part of automated safety instrumented system. Human factors can present limiters when designing human-machine interfaces. Although the automated safety instrumented system is intended to be a stand-alone system that automates responses of DCSs and WCSs during an uncontrolled loss of well stability, there will be a need for audible and visual warnings. The warnings should occur prior to the system initiating automated responses to allow the equipment operator time to intervene.

5.2.6.3 What We do Today

A combination of manual and automated tasks are used to activate the DCS and WCS to effectively shut in a wellbore. Human-machine interface interaction is required to initiate the shut-in process. Some individuals may be affixing manually handled equipment such as full open safety valves, while other individuals may be performing tasks to manually close a WCS or initiate a safety sequence.

5.2.6.4 Technology for Training Tomorrow (Simulators, etc.)

Drilling simulators are currently available and offer immersive environments. Simulators can offer detailed and realistic scenarios to teach vertical and horizontal drilling techniques, well control techniques, and safe operation in a virtual environment. Simulators should include equipment training inclusive of basic and complex work procedures. Competence assessments should be included. Simulation equipment should be adaptable to multiple configurations. Simulators should have the capability to train users to prevent, recognize, and resolve well control issues. In the event the issue cannot be resolved, the automated activation of the DCS and WCS should also be included in the training. Training should include both a successful and unsuccessful deployment of the automated safety instrumented system. Scenarios should also include decision based consequential learning capabilities.

6 Existing Technologies

6.1.1 General

A multitude of technologies exist for controlling the unexpected release of wellbore fluids. Technological advancements within the industry are in various stages of development and reliability. The continued development and use of the best available and safest technologies can lead to the early detection and automated response to well control events.

6.1.2 Electronic Drilling Recorders and Pit Volume Totalizers

6.1.2.1 Electronic drilling recorders, pit volume totalizers, and their data inputs are necessary for an automated system equipment envelope. These systems are the primary components that provide the indications that the wellbore is becoming unstable.

6.1.2.2 EDRs and PVTs have been evolving and provide the means for an early kick detection system. Early kick detection system platforms can be developed with machine learning, user input, or any combination thereof.

6.1.2.3 Early kick detection systems are being introduced within the industry to provide early warning indications that the well is becoming unstable. These complex, algorithmic systems target identification on smaller scales and faster than rig personnel typically are able to identify.

6.1.2.4 These systems are the primary component for all subsequent automated activities and equipment associated with bringing the well to a safe state.

6.1.3 Managed Pressure Drilling

6.1.3.1 MPD systems can achieve full automation to successfully detect and dynamically control an influx. Dynamic control of the influx can include the subsequent circulation of the influx out of the wellbore.

6.1.3.2 While conventional well control capabilities remain fully functional, MPD enables a response that may preclude their use and provides data for a more informed well control response. This improves safety and reduces the risks and costs associated with fighting kick/loss cycles, wellbore instability, and stuck pipe.

6.1.3.3 With MPD, when kicks occur, they are typically identified more quickly. Using MPD, the driller can change pressure on demand quickly and efficiently, instead of having to alter the mud weight. By detecting and reacting to problems before they become difficult or impossible to control, MPD can actively influence the safety and efficiency of rig operations.

6.1.3.4 In MPD operations, a closed-loop system enhances safety and efficiency compared to a traditional atmospheric mud return system by enabling wellbore pressure management. Every closed-loop and atmospheric mud system incorporates an RCD. Additional standard components include flow metering technologies, MPD choke manifold, downhole isolation valves, and sophisticated software and controls that integrate all components into one automated system.

6.1.3.5 Newly developed pressure control systems, which include a setpoint choke, reduce the manpower typically required for choke operation by providing semiautomatic pressure control. The integrated system enables basic MPD, flow drilling and underbalanced drilling. The user inputs the pressure set point, and the system automatically maintains pressure by applying constant BHP during drilling operations or connections. Compared to conventional manual and hydraulic chokes, the system provides more accurate and precise pressure control.

6.1.4 Automated BOP Closure Systems

6.1.4.1 Technology is currently under development to apply control logic to monitor, warn and act based on the sensor inputs. Warning of personnel, spacing out the drill string, shutting down the mud pumps, turning off top drive or kelly drive rotation, and closing an annular blowout preventer or shearing drill pipe using a shear ram are examples of potential applications once drilling and well control systems integration is achieved.

6.1.4.2 For an automated system, warning of personnel should be considered as an integral part of the system. It is important for personnel to be forewarned that certain equipment functions are about to automatically function based on the automated system processes and responses to a detected influx. At a minimum, warning systems should include audible and visual alarms. Other forms of warning systems are acceptable such as haptics which alert the user (e.g., vibrations, motions).

6.1.4.3 For an automated system, the drawworks should be included in the automated equipment envelope. The drawworks should be able to space out and position the drill string tool joint at the rig floor height while allowing the use of the proper BOP to secure the well.

6.1.4.4 For an automated system, the mud pumps should be included in the automated equipment envelope. This process in automation needs the pumps to remain on and at current output rates as the drill string is being hoisted to a safe spacing height. This should maintain the equivalent circulating density (ECD) until it reaches that set point to minimize influx. Once this process has occurred, the pumps should then be shut off. In some circumstances there may be trapped pressure. The automated SIS should bleed this pressure without manual intervention.

6.1.4.5 For an automated system, the top drive or kelly should be included in the automated equipment envelope. It is important to take measures to minimize chances of pack off or stuck pipe. This would minimize the chances of a pack off or stuck pipe situation as the string is being hoisted and the pumps are being turned off. This is possible with rig systems with top drives. A kelly (legacy) rig would need a stand-alone controller to turn the rotary table off.

6.1.4.6 Consideration should be given for flow check procedures within an automated system. Flow checks can be performed when indications are suspected or present. These similar indications are the primary driver for the automated system. As such, one should consider how or if time for a flow check should be incorporated into the system prior to the automated system closing in the well.

6.1.4.7 The system should be configured by the contractor and operator to align with the agreed upon BOP, valve, and choke manifold configurations.

6.1.4.8 The system should be configured by the contractor and operator to align with the agreed upon shut in procedures. These procedures can vary from wellsite to wellsite.

6.1.4.9 Some operations may have shear rams within the BOPs. For these instances, the shut-in procedures may need to include an option to incorporate the shear rams into the automated system. In this case, the system would need to be configured such that the other preventers are closed first before activation of shear rams.

6.1.4.10 Because there are many ways for false positives to inadvertently enable an automated system to shut in the well, a manual override feature should be considered as part of the design. If an override feature is enabled it should be clearly indicated. This manual override feature could also provide options for instances such as

a) bypassing BOP closure sequences,

b) activating shear rams, or

c) preventing the automated system from closing in the well altogether.

6.1.4.11 Logging all automated system events should be considered within the system. These can be captured either onsite, offsite, or both. Logging key information regarding the events, automated actions, and manual overrides should be considered as an inherent part of the design for subsequent investigations, analysis, and design changes.

7 Risk-based Approach to Implementation

7.1 Objective

Discussion of the various means by which the industry can achieve widespread implementation.

7.2 Description

A risk-based engineering and operation approach is highly recommended for the implementation of an automated safety instrumented system. The risks associated with the changes imposed by adding an automated SIS and the reliability of the system to sense, decide, and act to bring a well to safe state from an unplanned influx should be evaluated. If the implementation strategy fails to establish effective means to manage the impact of the associated changes, elevated levels of risk will be introduced adversely affecting the health and safety of personnel, environment, and assets.

The risk-based implementation strategy should include the following:

a) auxiliary equipment and interfaces;

b) risks with aging infrastructure;

c) human factors including HMI;

d) personnel qualification and competency;

e) hazard and operability study including failure mode and effect analysis;

f) recovery and emergency response planning.

The implementation of an automated safety instrumented system should consider input from the lease operator, drilling contractor, original equipment manufacturer, and service providers interacting or interfacing with these systems as part of their technology and service delivery.

8 Safety Instrumented System

8.1 Safety Integrity Level

A Safety Integrity Level (SIL) defines the probability of failure on demand that is required to achieve a specific safety objective. Multiple factors contribute to SIL's performance requirements that determine the levels, SIL 1 to SIL 4 with 4 being the highest level that can be achieved and is not defined for use in the process sector per IEC 61511. Key to any SIL calculation is the Probability of Failure on Demand (PFD) that is a quantitative probability number that identifies the dangerous failure of a safety function at the moment the function is required to perform. PFD calculations include variables such as,

a) Failure rates of each of the components that make up a SIF including failure modes;
b) Device redundancy including common cause failures;
c) Mean Time to Repair (MTTR);
d) Proof testing frequency (both online and offline); and
e) Detectable and undetectable dangerous and undangerous failures.

The other key consideration that goes into the calculation of a SIL is design consideration of a SIS, most notable is the separation of SIS from the existing Basic Process Control System (BPCS). Separation can include factors such as separate instruments, independent wiring and dedicated Logic Solvers and their associated I/O. Operators such as rams and annulars as well as devices such as valves that have years of proven in-field operational data can also be integrated into the performance calculation of a SIF. It is therefore acceptable for the convergence of SIS and the BPCS to be achieved at non-SIL rated final control elements and operators, if failure calculations of those components are performed. It should be noted that a common misconception is the assumption that the straight combination of specific SIL ratings in a SIS will yield the required SIL rating, i.e., the use of SIL 3 components in a SIF does not automatically yield a SIL 3 SIF. In general, SIL rated components have conditions associated with them that must be met to qualify for their SIL rating. An example is a SIL 3 rated pressure transmitter that can only be rated to SIL 3 if two are used in parallel.

Although some organizations consider the BOP control system as a SIS, it lacks the proper documented credentials required to appropriately designate the system as a SIS. It should also be noted that it is acceptable to include a person in the loop for a SIS operation for specific functions as long as they are defined in the SRS, the person is qualified to make decisions that may suspend the operation of a specific function due to operational requirements, and that they are modelled in the reliability analysis.

For BOP systems, specific functions should be considered for SIL rating and not the entirety of the BOP. As discussed in section 5.2.1, SIFs are an outcome of a collaborative effort between the key stakeholders. SIFs should be designed for their specific intended operation therefore no blanket SIL rating can accomplish the required risk reduction. Only after a SIF has been identified and quantified, should the design work begin that includes component selection and integration and the overall architecture of the SIS. Differentiating between the varieties of influx types should also be a component of the SRS and if required, a SIF for each type should be established.

SIS implementation should supplement robust and comprehensive alarm management techniques. Alarms allow the driller to make critical decision during operations prior to any hazardous event. A SIS should only be activated should a process reach a state that violates safety conditions.

Bibliography

[1] API Specification 16C, *Choke and Kill Equipment*

[2] API Standard 53, *Well Control Equipment Systems for Drilling Wells*

[3] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[4] IEC 61511 (all parts), *Safety instrumented systems for the process industry sector*

[5] IEC 62443 (all parts), *Industrial communication networks – Network and system security*

[6] ISA-84 (all parts), *Functional Safety: Safety Instrumented Systems For the Process Industry Sector*

[7] ISA-TR84, Part 2 - Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations