GAP Analysis

Safe Influx Automated Well Control System
vs.
API Bulletin 16H

Document Number	SATECR074			
Revision	**Issue Date**	**Prepared by**	**Reviewed by**	**Approved by**
Final Revision	23/05/2022	Mark Gillard, Muhammad Abbas Bhatti	Bryan Atchison, Juliana Bond	Bryan Atchison

Safe Influx Ltd.
Bryan Atchison, Managing Director, bryan.atchison@safeinflux.com
+44 (0) 7912 242421

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 1

Table of Contents

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H,
First Edition, February 2022 – Final Revision

Page 2

1. Purpose

The purpose of this report is to present the findings of a formal GAP analysis of the Safe Influx Automated Well Control system and API Specification 16H – Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation (First Edition, February 2022).

The API 16H bulletin provides information on existing and emerging technologies that could be integrated to bring a well to a safe state in the event other operational barriers fail. The bulletin discusses strategies to create an automated blowout preventer actuation system, the challenges and obstacles associated with these types 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 if the site personnel do not recognize a well influx or are unable to respond to one. The implementation of an automated safety instrumented system should consist of input from the lease operator, drilling contractor, and original equipment manufacturer.

Because the Safe Influx Automated Well Control system is the current technology and forms a part of the well control logic, a review of this specification was considered necessary to ensure that no specific conflicts with API 16H Bulletin are noted and that a claim of largely compliant could be supported.

Compliance	*manufactured or produced in accordance with a specified body of rules (usually used in combination).*

According to this definition, it is concluded that the Safe Influx Automated Well Control system is fully compliant with the API 16H guidance and information (as detailed in Section 6)

2. Overview

The Automated Well Control system has been developed by Safe Influx enabling safe closure of a well whilst drilling.

Pre-determined influx rates, agreed by the operator and drilling contractor, and input by the driller are established. Once the automated system detects the influx, it performs a series of operations by taking control of the drilling rig equipment and closing the BOP without human intervention.

Safe Influx system is currently designed to work in the drilling phase of a well. Several additional modules have been conceptualised to enhance safety performance as the industry increasingly embraces the use of automation.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 3

3. GAP Analysis Methodology

The GAP analysis is focussed on documentation, processes, and procedures to ensure the Automated Well Control system has been built and deployed in accordance with API 16H Bulletin.

The governing criterion of this exercise is to ensure that the Safe Influx Automated Well Control system has been designed, built, deployed, and operated within the criteria established by industry.

The colour code detailed in Table 1 is employed for easy identification of the status of each of the line items in API 16H and details the general criteria for assessing any gaps between the relevant documents and procedures.

Acceptable	Complies	Full **compliance** with the statements in API 16H.
	Conforms	This categorisation is applied to items that conform to the spirit of the API 16H statement but are not necessarily **compliant** with the specification.
	Considered	Where some relevance to Automated Well Control systems is perceived, **consideration** will be given to the relevant section of API 16H.
	Consulted	Several additional documents will be **consulted** during the GAP analysis. Where documents are explicitly cited in API 16H but are not considered directly relevant, this category will apply
	Future Module	This categorization is applied when the subject matter is **considered** and **future modules** have already been conceptualized.
	Not Applicable	Items categorized as **Not Applicable** are API16H statements that refer to elements that are not relevant to Automated Well Control Systems
Not Acceptable	Action	An **action** that needs to be executed to ensure compliance/conformance with API 16H or to apply a Not Applicable category.
	Issue	**Non-compliance** with API 16H.

Table 1 - Colour Coding for GAP analysis.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 4

Where there is doubt about compliance or conformance to statements in API 16H, the gap is highlighted as a <u>presumption</u> of non-compliance, until proven otherwise and where there is an issue or action associated with a statement in API16H, a corresponding action is generated for completion.

The colour code detailed in Table 2 is employed for easy identification of the responsible parties.

Responsible Parties
Safe Influx
System Manufacturer
OEM
Customer
Drilling Contractor
Not Applicable

Table 2 - *Colour Coding for responsible parties.*

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 5

4. Relevant Documents

Reference should be made to Appendix 1, which has been prepared to facilitate the GAP analysis.

The following Safe Influx and Finesse documentation is referenced during the GAP analysis.

Document Number	Contents
	API Bulletin 16H - Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation (First Edition, February 2022)
SATEC060	Product Assurance Statement
SATEC065	False Positive Indicators – Management Strategy
FATECD003	Functional Design Specification MVP; P7048 Doc 001 revA2-MVP-FDS 29-1-2019
	Functional Failure Modes and Effects and Analysis (MPD) 02-Sep-20
	Lloyds Register Technical Qualification Certificate(s) 16-Apr-2019
FATECP001	Software Configuration Management Procedure (FCS QP11-R5)
FATEDS004	Component Description (7048- Doc- 008)
FATECD007	Electrical Schematics MVP (7048-DWG-001)
FATECP009	Mean Time Between Failure (MTBF) (X7048-DOC-9-R0)
SATECP005	Factory Acceptance Test Procedure 2019
SATECP006	Site Acceptance Test Procedure
SATECM021	Operator Manual Conventional Rig System - Surface BOP (Conventional)
SATECM021	Operator Manual Conventional Rig System - Surface BOP (Cyber)
SATECM021	Operator Manual Conventional Rig System - Surface BOP (MPD)
SXFCSF039	Software Change Request Form

Links to these documents can be shared with stakeholders on request.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 6

5. GAP Analysis

The API 16H is composed of eight sections and the analysis was done for each of these sections in the order below:

5.1 Scope

This section presents the Scope of API 16H Bulletin that provides a list of the equipment and interfaces to be considered for the automation of blowout preventer closure to place the well in a safe state in an **onshore** environment.

This section also 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;
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) Logic solvers;
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) Pit level sensors

Automated Well Control sequence for the current Minimum Viable Product:

1. The system receives **a kick indicator signal** from the **flowmeter** (drilling ahead) or **MPD controller** (MPD Module)
2. The system initiates an audible alarm signal
3. The system sends a warning message to the driller "Auto Well Control Initiated".
4. The system takes control of the assigned rig equipment and performs the following automated sequence:
   a. Continues pumping and rotating whilst picking up the drill string using the **draw works** to the first available safe space out location.
   b. Stop **mud pumps** and **top drive** rotary motion.
   c. Monitor flow from well. If flow continues, shut in the well.
   d. Activate **BOP** to shut in the well
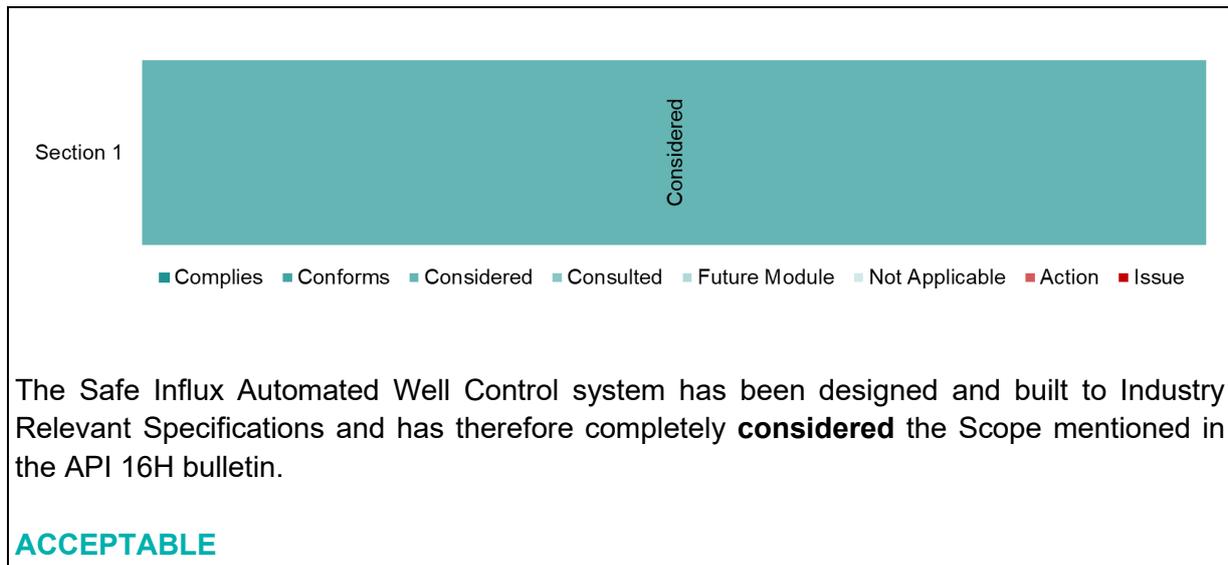
Figure 1 GAP Analysis - Scope.

The Safe Influx Automated Well Control system has been designed and built to Industry Relevant Specifications and has therefore completely **considered** the Scope mentioned in the API 16H bulletin.

ACCEPTABLE

5.2   Normative References

There are no normative references in the document

Section 2 is **not applicable** to the Safe Influx Automated Well Control system

ACCEPTABLE
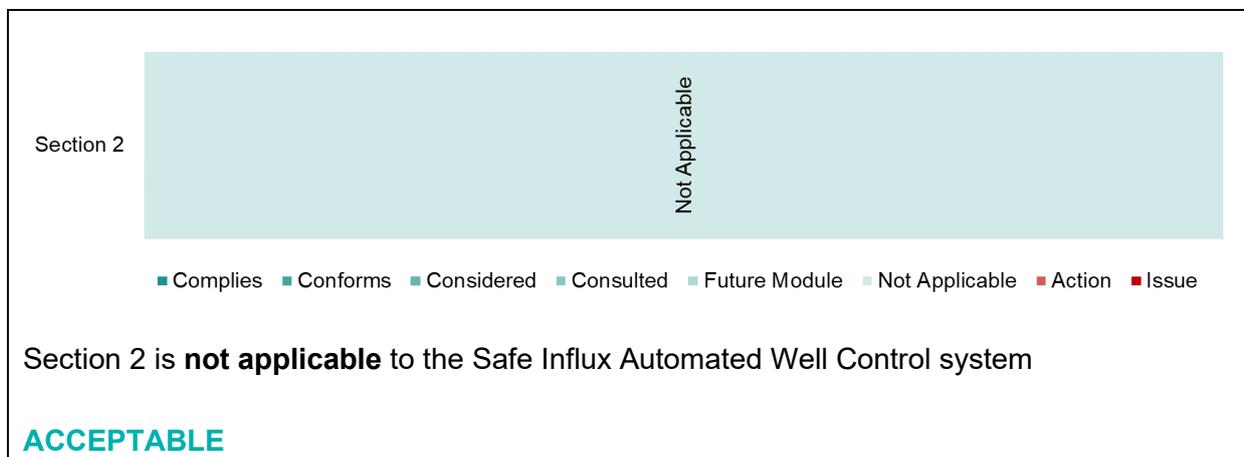
Figure 2 GAP Analysis - Normative References.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 8

5.3 Terms, Definitions and Abbreviations

This section presents the terms, definitions and abbreviations applied for the purpose of the API 16H.

The contents of Section 3 have been **consulted** when performing the GAP Analysis

ACCEPTABLE
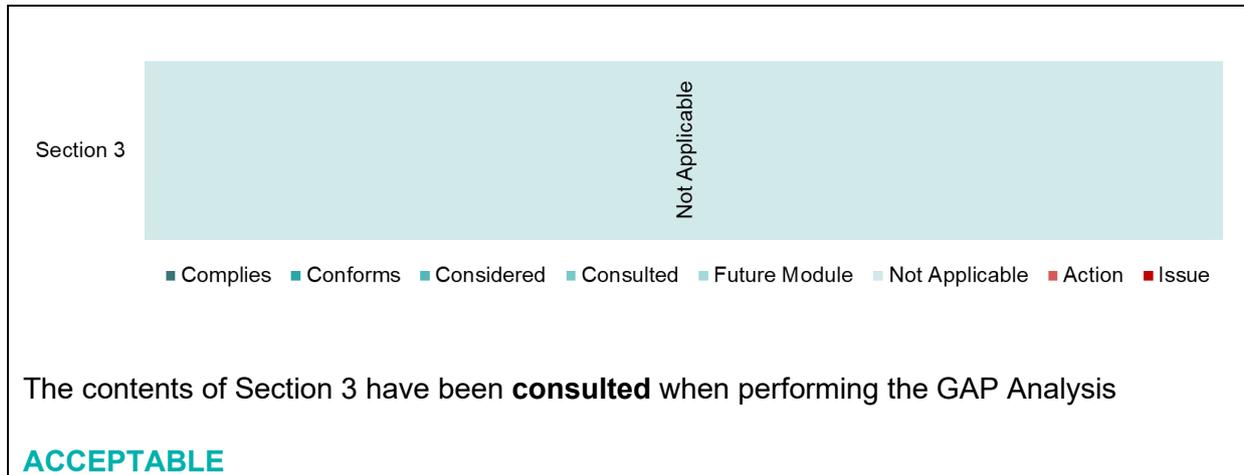
Figure 3 GAP Analysis - Terms, Definitions and Abbreviations.

5.4 Key Elements of Automated Safety Instrumented Systems

This section discusses key elements of Safety Instrumented System that need to be considered when designing, testing, and implementing a system that can automate the process of bringing a well to a safe state by shutting in the blowout preventer (BOP).

This section is further broken down into to 4 different sections with further sub-sections:

1) Monitoring Equipment.
2) Logic Solver Types
3) Equipment Under Control
4) Operational Controls.

These categories were individually assessed to determine the applicability into a Safety Instrumented System (SIS). Original Equipment Manufacturers (OEM), lease operators, and drilling contractors to evaluate the individual and combined components of an SIS.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 9

Analysis:

The design and manufacture of the Automated Well Control system **complies** with 18% of the elements in API 16H. This includes flowmeters, PLCs, Human detection and actions during influx detection, the process to close the BOP, and well control procedures. **Conformance** is applied to 6% of the elements

44% of the elements in API 16H have been **considered** during the development phase which includes the equipment under control (Top drive, drawworks, mud pumps and BOP). 2 **Future Modules** have been conceptualised because of this consideration

32% of the elements were **not applicable** to the Automated Well Control system and were directed towards different logic solvers, different indicators, and irrelevant well control systems which are not directly applicable to the current Safe Influx Automated Well Control system and will be considered in future modules.

ACCEPTABLE

Figure 4 GAP Analysis - Automated Safety Instrumented Systems.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 10

5.5 Obstacles and Challenges

This section discusses the obstacles and challenges in the introduction of emerging technologies such as those utilized to develop automated safety instrumented systems.


Analysis:

The design and manufacture of the Automated Well Control system **complies** with 85% of the elements in API16H **(**focused on Automated BOP Actuation)

This observation also includes compliance with proprietary software, intellectual property, dealing with false positives and negatives, cyber security, site integration and user acceptance testing, as well as human factors covering HMI design, training, audible and visual alarms

15% have been **considered** or **consulted** demonstrating that the spirit of the API 16H specification is acknowledged. This includes working with multiple original equipment manufacturers (OEMs) and endurance and performance testing.

ACCEPTABLE

Figure 5 GAP Analysis - Obstacles and Challenges.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 11

5.6 Existing Technologies

This section discusses a multitude of technologies that exist for controlling the unexpected release of wellbore fluids. It is noted that technological advancements within the industry are in various stages of development and reliability.

This section is further broken down to 3 different categories with further sections, sub-sections, and index:

1. Electronic Drilling Recorders and Pit Volume Totalizers.
2. Managed Pressure Drilling.
3. Automated BOP Closure Systems.

Analysis:

The design and manufacture of the Automated Well Control system **complies** with 52% of the elements

Additionally, 26% (7) of the API 16H elements are covered under the Safe Influx module development process and are therefore classified as **future modules** which have been already conceptualized.

19% of the elements can be classified as **conforms** which includes the statements mentioned under the Managed Pressure Drilling heading in section 6.1.3

4% of the elements were **not applicable** to the Automated Well Control system.

ACCEPTABLE

Figure 6 GAP Analysis - Existing Technologies.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 12

5.7   Risk-based Approach to Implementation

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 Safety Instrumented System 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.

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.


Analysis:

The design and manufacture of the Automated Well Control system **complies** with 100% of elements described in API16H with respect to the risk- based engineering operations approach for the widespread implementation of the automated safety instrumental systems.

Reference should be made to the following documents:

SATEC060   Product Assurance Document
Comparative Human Factors Analysis – Marex Marine and Risk Consultancy

ACCEPTABLE
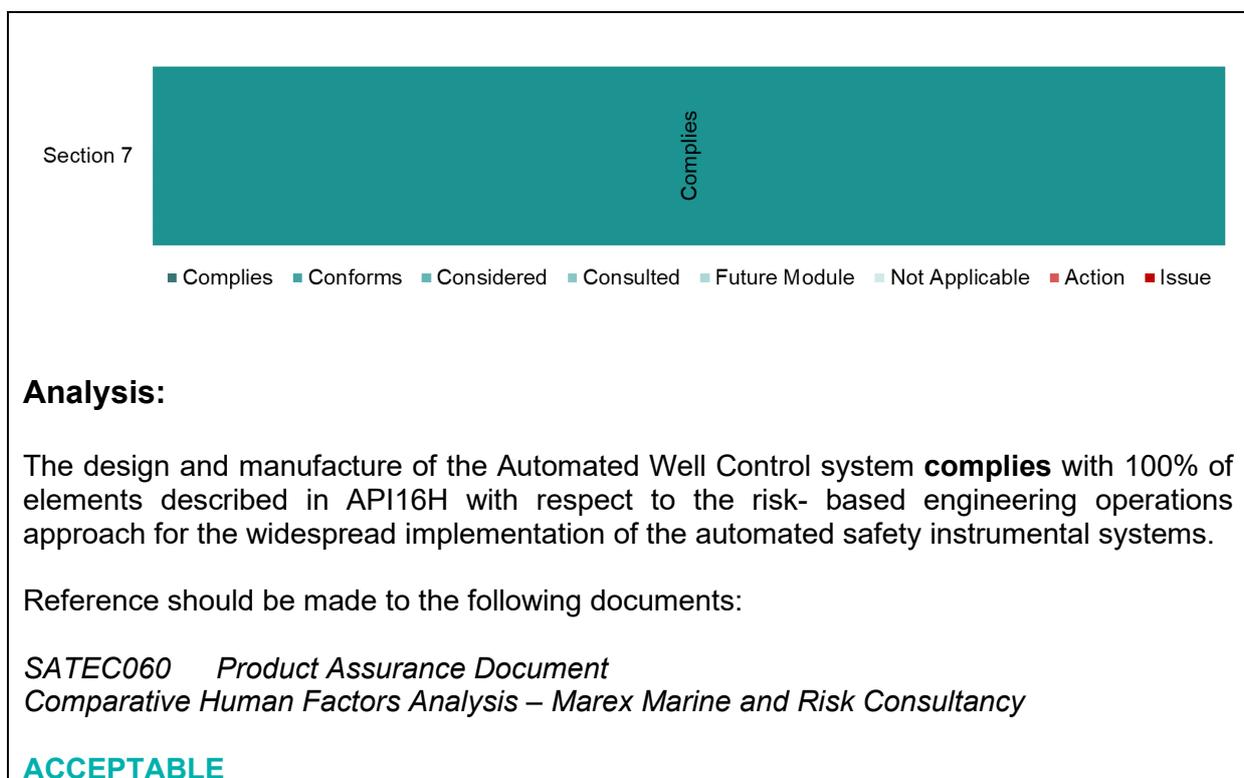
Figure 7 GAP Analysis - Risk Based Design Approach.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 13

5.8   Safety Instrumented System

This section details the Safety Integrity Level (SIL) of Safety Instrumented Systems (SIS). A SIL rating defines the probability of failure on demand that is required to achieve a specific safety objective.

Key to any SIL calculation is the Probability of Failure on Demand (PFD) – 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 SIS 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 failure

Analysis:

The Automated Well Control System is rated as *SIL2*, dependent upon the quality of equipment it interfaces with, and conforms to several quality assurance protocols. The design and manufacture of the Automated Well Control system therefore **complies** with 100% of elements described in API16H with respect to the specification mentioned in the Safety Integrity Level of the Safety Instrumented systems.

ACCEPTABLE
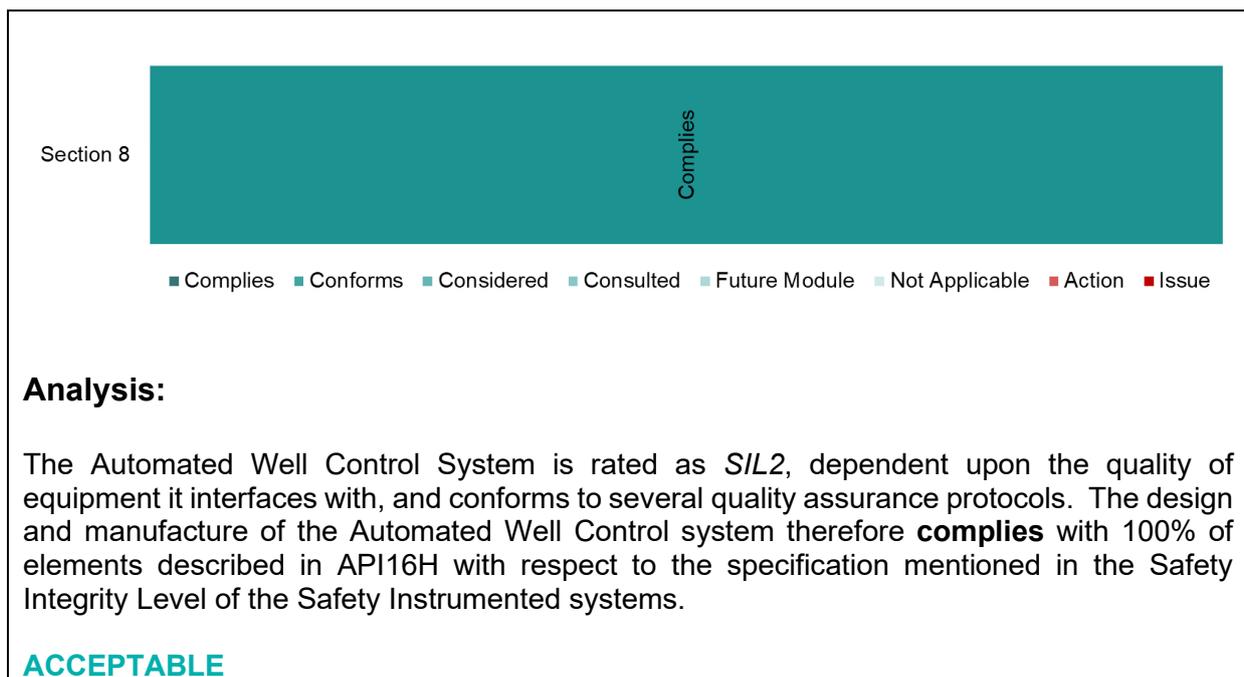
Figure 8 GAP Analysis - Safety Instrumented Systems.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 14

6. Conclusion

The object of this GAP analysis was to ascertain whether the Safe Influx Automated Well Control system is compliant with API Bulletin 16H.

Given that compliance can only be applied to a 'specified body of rules', a sliding scale of conformity was used **(Table 1**) to ensure that the GAP analysis was performed to a pre-agreed criteria set within the outlines of the recently published Bulletin.

API specifications are intended to 'facilitate the broad availability of proven sound engineering and operating practices' a measure of conformance to API16H can be applied.

It is concluded that detailed studies, risk assessments and industry learnings applied to the design and manufacture of the Safe Influx Automated Well Control system shows no significant GAPS to the guidance provided in the Bulletin and that the claim of compliance is justified.

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 15

Appendix 1 GAP Analysis

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H,
First Edition, February 2022 – Final Revision

Page 16

Gap Analysis - Safe Influx Automated Well Control and API Bulletin 16H (First Edition, February 2022)
API Bulletin 16H - Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
	1					**Scope**	Considered	Safe Influx	
		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	Considered	Safe Influx	
		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; 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) Logic solvers; 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) Pit level sensors	Considered	Safe Influx	The Safe Influx Automated Well Control Systems have been designed and built to Industry Relevant Specifications, API 16H has been consulted (in the context of Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation)
		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	Considered	Safe Influx	
	2					**Normative References**	Not Applicable	Not Applicable	
						There are no normative references in this document.	Not Applicable	Not Applicable	
	3					**Terms, Definitions, and Abbreviations**	Not Applicable	Not Applicable	
		3.1				Terms and Definitions : For the purposes of this document, the following terms and definitions apply.	Not Applicable	Not Applicable	
			3.1.1			**black channel** A communication channel with unsecured properties or properties that do not fit the application	Not Applicable	Not Applicable	
			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.	Not Applicable	Not Applicable	
			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.	Not Applicable	Not Applicable	
			3.1.4			**bottom-up integration testing** Testing the lowest units of the application and gradually moving up one-by-one	Not Applicable	Not Applicable	
			3.1.5			Missing	Not Applicable	Not Applicable	
			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.	Not Applicable	Not Applicable	
			3.1.7			**equipment under control** The set of all equipment, machinery, apparatus or facility that gives rise to hazardous events for which the safety-related system is required	Not Applicable	Not Applicable	
			3.1.8			**false negative** An indication that an event is absent when one occurs	Not Applicable	Not Applicable	
			3.1.9			**False positive** An indication that an event is present when one does not occur	Not Applicable	Not Applicable	
			3.1.10			**kick** Intrusion of formation fluids into the wellbore	Not Applicable	Not Applicable	
			3.1.11			**pipe tally** The current total number of drill pipes (including the bottom-hole assembly) in use	Not Applicable	Not Applicable	
			3.1.12			**programmable logic controller (PLC)** A microprocessor-based device capable of controlling many types of industrial equipment and entire automated systems	Not Applicable	Not Applicable	
			3.1.13			**remote telemetry unit (RTU)** A microprocessor-based device connected to sensors, transmitters, or process equipment for the purpose of remote control	Not Applicable	Not Applicable	
			3.1.14			**remote terminal unit** A multipurpose device used for remote monitoring and control of various devices and systems for automation	Not Applicable	Not Applicable	
			3.1.15			**safe state** The state of the process after acting to mitigate the hazard	Not Applicable	Not Applicable	
			3.1.16			**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	Not Applicable	Not Applicable	
			3.1.17			**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.	Not Applicable	Not Applicable	

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
			3.1.18			**supervisory control and data acquisition (SCADA)** 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	Not Applicable	Not Applicable	
			3.1.19			**top drive** A device that can be hoisted in the derrick or mast of a drilling rig that rotates the drillstring	Not Applicable	Not Applicable	
			3.1.20			**top-down integration testing** Testing the top-most modules and gradually moving down to the lowest set of modules one-by-one	Not Applicable	Not Applicable	
			3.1.21			**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	Not Applicable	Not Applicable	
		3.2				**Abbreviations**	Not Applicable	Not Applicable	
						AI Artificial Intellignece BPCS Basic process control system BHP bottom-hole pressure BOP blowout preventer DCS drilling control system EDR electronic drilling recorders FSMP Functional safety management plan HMI human machine interface IP Intellectual Property MPD managed pressure drilling OEM original equipment manufacturer PFD Probability of failure on demand PLC programmable / process logic controller PLR programmable logic relay PVT pit volme totalizer RCD rotating control device RTU remote telemetry unit SIF safety instrumented function SIL Safety Integrity Level SIS safety instrumented system SRS safety requirement specification SCADA supervisory control and data acquisition USB universal serial bus WCS well control system	Not Applicable	Not Applicable	
	4					**Key Elements of Automated Safety Instrumented Systems**	Considered	Safe Influx	
		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 blowout preventer (BOP)	Considered	Safe Influx	
		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 a 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.	Considered	Safe Influx	
		4.3				**Description**	Conforms	Safe Influx	
			4.3.1			**Monitoring Equipment**	Conforms	Safe Influx	
				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.	Future Module	Not Applicable	
				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 . This method typically consists of equipment such as a rotating control device (RCD) and MPD choke manifold, depending on the application .	Considered	Not Applicable	
				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.	Complies	Safe Influx	The Automated Well Control system receives a kick indicator signal from the flowmeter (drilling ahead). If there is a positive kick, increase in the flowrate triggers the Automated Well Control sequence.
				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.	Future Module	Safe Influx	PVT sensors are of course a primary indicator, but it is delayed by the volume of the flowline so is always behind the flowmeter

Gap Analysis - Safe Influx Automated Well Control and API Bulletin 16H (First Edition, February 2022)
API Bulletin 16H - Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
				4.3.1.5		**Pipe Tallies** Pipe tallies are used in conjunction with the length to help the driller know the exact location of the	Not Applicable	Not Applicable	
					4.3.1.5.1	drill bit or other drill string component datum. They can be manual or automated tallies	Not Applicable	Not Applicable	
					4.3.1.5.2	Automated tallies typically use some type of technology to uniquely identify each drill pipe such as 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.	Not Applicable	Not Applicable	
					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 wellbore.	Complies	Safe Influx	Logic Relying document
			4.3.2			**Logic Solver**	Not Applicable	Not Applicable	
				4.3.2.1		**Supervisory Control and Data Acquisition** Supervisory control and data acquisition (SCADA) systems utilize programmable logic controllers (PLCs), remote terminal units, or similar technologies. These microprocessor-based systems collect information about a well control system and are capable of controlling the shut-in operation.	Not Applicable	Not Applicable	
				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	Complies	System Manufacturer	High availability and Safety Siemens S7/412 FH CPU x 2 (or Equivalent).
				4.3.2.3		**Programmable Logic Relays** Programmable logic relays are similar in functionality to PLCs, although they have limited scalability.	Not Applicable	Not Applicable	
				4.3.2.4		**Discrete (Relay) Logic Control System** Discrete logic control systems are hard wired control systems that uses instrumentation, switches, timers, relays, contractors, motors and actuators.	Not Applicable	Not Applicable	
				4.3.2.5		**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.	Not Applicable	Not Applicable	
			4.3.3			**Equipment Under Control**	Considered	Safe Influx	
				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 equipment in sections 4.3.3.1.1 through 4.3.3.1.3.	Complies	Safe Influx	Safe Influx is performing various integration and collabration test with few of the biggest drilling control systems provider that are normally tight about introducing external inputs into their systems.
					4.3.3.1.1	**Top 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	Considered	Safe Influx	Top Drive is the part of the Automated Well Control Logic sequence.
					4.3.3.1.2	**Drawworks** Drawworks are hoisting mechanisms, or winch, used to spool the hoisting cable in a controlled fashion.	Considered	Safe Influx	Drawworks is the part of the Automated Well Control Logic sequence.
					4.3.3.1.3	**Mud Pumps** Mud pumps are used 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.	Considered	Safe Influx	Mud Pumps are the part of the Automated Well Control Logic sequence.
				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 in sections 4.3.3.2.1 through 4.3.3.2.5..	Considered	Safe Influx	Safe Influx will perform various integration and collabration test with few of the biggest well control systems provider i.e. Hydril, Cameron etc.
					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 use 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 uses 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.	Considered	Safe Influx	BOP is the part of Automated Well Control Logic sequence.

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
					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.	Not Applicable	Not Applicable	
					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.	Not Applicable	Not Applicable	
					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. Remote control valves typically receives a fluid signal through the pilot line to operate the selected function	Not Applicable	Not Applicable	
			4.3.4		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 interactionwith push-button or touchscreen interfaces.	Considered	Safe Influx	Safe Influx has considered the BOP Control Systems during the development of Automated Well Control. Push and hold button to close the BOP also forms the part of the Logic.
				4.3.4.1		**Operational Barriers** **Hydrostatic Pressure** Hydrostaticpressure 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.	Considered Considered	Safe Influx Safe Influx	Considered during the development phase.
				4.3.4.2		**Human Detection and Action** Human senses such as sight, smell, sound, and touch can 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	Complies	Safe Influx	Safe Influx's Automated Well Control technology, in its current form, detects a kick, takes control of the rig equipment to space out, shuts down the mud pumps and top drive, and then shuts-in the BOP. It has significant potential and application in the industry to manage/reduce well control risks & associated impacts
				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 can be considered when designing automated blowout prevention equipment and systems capable of bringing a well to a safe state from a kick.	Complies	Safe Influx	It depends what the client wants. Each rig installation will be carefully surveyed and a bespoke engineered solution for every rig will be provided. If the client wants additional information fed in from a mud-logging or other company, we have the ability to accept that feed. One of our future upgrades is to develop a multiple data source input into an algorithm. It would accept the two primary indicators of a kick and multiple secondary indicators. An algorithm would be constantly polling these indicators.
	5					**Obstacles and Challenges**	Complies	Safe Influx	
		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. SIS, if not integrated properly, can result in reduced operational efficiency, increased downtime, operational risk, and potential loss of assets.	Complies	Safe Influx	Automated Well Control will help to mitigate the blowouts and kicks cause due to human factors and organisational issues in a timely, efficiently and cost effective manner.
		5.2				**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 SRS contains the necessary functional and performance requirements to achieve a safe state shutdown for each SIF in accordance with IEC 61511. 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	Complies	Safe Influx	

Gap Analysis - Safe Influx Automated Well Control and API Bulletin 16H (First Edition, February 2022)
API Bulletin 16H - Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
			5.2.1			**Integrating and Modifying Systems**	Complies	Safe Influx	
				5.2.1.1		**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.	Complies	Safe Influx	Automated Well Control is the property of Safe Influx Ltd.
				5.2.1.2		**Intellectual Property** 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.	Complies	Safe Influx	To protect Intellectual property (IP), the Safe Influx Automated Well Control system has been granted a patent in the United Kingdom to cover the 'drill ahead' base product (drilling and tripping) and 34 additional modules to cover the entire well construction lifecycle. Patents are pending in United States of America (expected award: Q2 2022) and Europe, Canada, and Australia(expected award: 2024).
				5.2.1.3		**Working with Multiple OEMs** When multiple original equipment manufacturers are involved, a principal contractor should be selected. The principal should establish a sytems engineering approach for the design, method, and process changes based on agreed requirements.	Considered	Safe Influx	STAMP Process to be used
			5.2.2			**Kick Detection System**	Complies	Safe Influx	
				5.2.2.1		**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 set-points and parameters can be utilized and machine learning capabilities can be incorporate . Additionally, kick detection systems help to reduce nuisance alarms that create alarm fatigue. Minimum and maximum parameters should be established to eliminate nuisance alarms as low as reasonably practicable (ALARP) or as low as reasonably achievable (ALARA) and to reduce potential alarm fatigue. The kick detection system can pose both false positive and false negative results within the instrumentation.	Complies	Safe Influx	False Positive Indicators Management Strategy Drilling Ahead Module
				5.2.2.2		**False Positives** False positive indicators from systems negatively impact trust from humans and therefore reduce the effectiveness of the system. Too many false positives can encourage the operators to disable the alarms to prevent reoccurrences. The system should be designed so false positives are kept to a minimum.	Complies	Safe Influx	False Positive Indicators Management Strategy Drilling Ahead Module
				5.2.2.3		**False Negatives** 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.	Complies	Safe Influx	False Positive Indicators Management Strategy Drilling Ahead Module
				5.2.3		**Cybersecurity** As with any computer-based system, security is a key element in system reliability. As the criticality of a system increases, the need for cybersecurity to be designed into the system also increases. 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. A 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 can also allow malicious changes to the system. Any external access to the system should be secured to prevent unauthorized system changes. Wherever possible, external access should be avoided to mitigate malicious changes to the system. 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.	Complies	Safe Influx	Safe Influx recognises the concern of operators and drilling contractors that essential well control equipment could be vulnerable to external hacking. At present, Safe Influx Automated Well Control technology does not have, nor does it rely upon, any connection to the internet or use of wireless technology thus significantly reducing the exposure to cyber-hacking. Future development of the technology will include modules that require it to connect to the internet. Such modules would allow remote troubleshooting, software updates and system monitoring to be established. Safe Influx will collaborate closely with the customer to ensure that the technology strictly adheres to relevant Cyber Security policies and international standards (IEC62443-4-1)

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
			5.2.4			**Testing**	Conforms	System Manufacturer	
				5.2.4.1		**Endurance and Performance Testing** Endurance or performance testing refers to tests performed to find out whether the system can withstand the processing load it is expected to endure for a pre determined time period. 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.	Conforms	System Manufacturer	Standard refers back to Siemens
				5.2.4.2		**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.	Complies	Safe Influx	Rig Survey Document
			5.2.5			**Human Factors**	Complies	Safe Influx	
				5.2.5.1		**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.	Complies	Safe Influx	

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
				5.2.5.2		**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.	Complies	System Manufacturer	There is a MUTE Tab at the bottom of each HMI Touch Screen. Visual and audible alarm initiates when an influx is detected. Audible alarm can be be muted via HMI screen by touching the MUTE Tab. Visual alarm remains active.
				5.2.5.3		**Human Machine Interface** 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.	Complies	System Manufacturer	Human Machine Interface Touch screen of 19" is positioned next to the driller. It is a user friendly design. Driller can take control of the drilling and well control equipement anytime he wants.
				5.2.5.4		**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.	Complies	Safe Influx	Visual Training is already availabe
	6					**Existing Technologies**	Complies	Safe Influx	
		6.1				General	Complies	Safe Influx	
						General			
			6.1.1			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 existing and emerging technologies can lead to the early detection and automated response to well control events	Complies	Safe Influx	
			6.1.2			Electronic Drilling Recorders and Pit Volume Totalizers	Future Module	Safe Influx	
				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.	Future Module	Safe Influx	The future Safe PVT module will measure the changes in the active mud pit volume sensors which is considered as a primary kick indicator.
				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.	Future Module	Safe Influx	Subject to pre-set criteria agreed between the Operator and Drilling Contractor, the EKDS module will process this information, along with information from other module sensors, accordingly
				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.	Future Module	Safe Influx	The Future Safe LinkEKDS module would link the Safe Influx system to a third party's Early Kick Detection System (EKDS) that the Operator or Drilling Contractor decides to have on the rig.
				6.1.2.4		EDRs and PVTs are the primary components for all subsequent automated activities and equipment associated with bringing the well to a safe state.	Future Module	Safe Influx	The future modules will take into account PVTs and EDRs.
			6.1.3			Managed Pressure Drilling	Complies	Safe Influx	
				6.1.3.1		MPD systems can achieve full automation to successfully detect and dynamically control an influx in some applications. Dynamic control of the influx can include the subsequent circulation of the influx out of the wellbore	Complies	Safe Influx	Callobration between Safe Influx Automated Well Control System and Weatherford MPD System.
				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.	Conforms	Customer	
				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	Conforms	Customer	
				6.1.3.4		In MPD operations, a closed-loop system enhances safety and efficiency compared with 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	Conforms	Customer	
				6.1.3.5		Pressure control systems that include a setpoint choke can reduce the manpower typically required for choke operation by providing semiautomatic pressure control. 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.	Conforms	Customer	
				6.1.3.6		While MPD can prove beneficial in assisting to manage well control events, not all the drilling operations are candidates for MPD. A risk analysis should be performed to determine if using MPD is appropriate for the well or operation.	Not Applicable	Not Applicable	

Gap Analysis - Safe Influx Automated Well Control and API Bulletin 16H (First Edition, February 2022)
API Bulletin 16H - Automated Safety Instrumented Systems for Onshore Blowout Preventer Actuation

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
			6.1.4			**Automated BOP Closure Systems** Automated BOP closure systems can 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 rotation, and closing an annular blowout preventer or shearing drill pipe using a shear ram, are examples of potential applications once DCS and WCS integration is achieved.	Conforms	Safe Influx	
				6.1.4.1			Complies	Safe Influx	Automated Well Control done all of it in a systematic and controlled fashion.
				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).	Complies	Safe Influx	Visual and audible alarm initiates when an influx is detected. Audible alarm can be be muted via HMI screen by touching the MUTE Tab. Visual alarm remains active.
				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.	Complies	Safe Influx	Drawworks is the part of the Automated Well Control Logic sequence.
				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	Complies	Safe Influx	Mud Pumps are the part of the Automated Well Control Logic sequence.
				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. An automated top drive can minimize the chances of a pack off or stuck pipe situation as the string can be rotated. A kelly rig would need a stand-alone controller to automate the rotary table functions.	Complies	Safe Influx	Top Drive is the part of the Automated Well Control Logic sequence.
				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.	Complies	Safe Influx	Time delay set points are incorporated to overcome any false indication.
				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.	Complies	Contractor	It depends what the client wants. Each rig installation will be carefully surveyed and a bespoke engineered solution for every rig will be provided based on the contractors and operators requirements.
				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.	Complies	Contractor	The current viable product follows the Hard Shut in procedure. If any Operator or contractor wants soft shut in procedure or others, it could be surveyed and agreed upon.
				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.	Future Module	Safe Influx	The future module would provide the ability to automatically assess the position of the tool joint in relation to the exact BOP ram configuration on the rig, and to then auto-select which is the best ram to close at any given time. Having the confidence to immediately close a ram (rather than an annular) in a deepwater situation could be very beneficial.
				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.	Complies	Safe Influx	Safe Influx Automated well control system allows the driller to immediately stop the closure process by a 'double tap' on the HMI interface in the case where late realisation of a false positive indication occurs. This veto prevents further action of the system and will halt the final process of well closure. In the case that the Veto command is issued, full control of the rig systems is reconnected to the driller. Re-arming of the automated system can only be done by resetting the Automated Well Control system.
				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	Future Module	Safe Influx	Data Logging will be an upgrade to current system.

Reference	Chapter	Category	Section	Subsection	Index	API16H	Status	Responsible Party	Comments
	7					**Risk-based Approach to Implementation**	Complies	Safe Influx	
					7.1	**Objective** Discussion of the various means by which the industry can achieve widespread implementation.	Complies	Safe Influx	
					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.	Complies	Safe Influx	All components used in the manufacture of the Safe Influx Automated Well Control System have been selected with quality and reliability in mind. For more information please look at the Product Assurance Statement document at the Safe Influx Website.
	8					**Safety Instrumented System**	Complies	System Manufacturer	
					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. Those requirements determine the SILs, which are designed SIL 1 to SIL 4, SIL 4 is 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 to be 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.	Complies	System Manufacturer	The Safe Influx Automated Well Control system has been manufactured using high quality components in compliance with the Safety Integrity Level 2 classification. In SIL 2 Compliance for demand use, the Probability of dangerous failure 0.01-0.001 and Risk Reduction Factor 100-1000 In SIL 2 compliance for continuous operation, the probability og dangerous failure per hour is 0.000001-0.0000001 and risk reduction factor is 1,000,000- 10,000,000. The minimum mean time between failure for control panel is 90.3 years and for HMI display is 7.99 years at 25°C. In most cases the SIL classification of the Safe Influx equipment exceeds the SIL classification of both the input and output phases of the rig's control system(s), meaning that the Automated Well Control System cannot be considered as the weakest link in the chain. FATECP009 Mean Time Between Failure (MTBF) (X7048-DOC-9-R0)Functional Failure Modes and Effects and Analysis (MPD) 02-Sep-20 and Product Assurance document for more details.
						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	Complies	System Manufacturer	

End of Document

This is a document produced by Safe Influx team. Wherever appropriate, the source of the data has been indicated. The document shall not be reproduced or transferred to other documents or disclosed to others or used for any purpose other than for which it is furnished without the prior written permission of Safe Influx Ltd.

Certificates and documents mentioned in this material are contained in a separate volume. If you would like access to those documents, do not hesitate to contact Safe Influx.

info@safeinflux.com
www.safeinflux.com

GAP Analysis Safe Influx Automated Well Control System vs. API Specification 16H, First Edition, February 2022 – Final Revision

Page 26