Standard for Subsea High Integrity Pressure Protection Systems (HIPPS)

API STANDARD 17O
SECOND EDITION, JULY 2014

AMERICAN PETROLEUM INSTITUTE

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.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Classified areas may vary depending on the location, conditions, equipment, and substances involved in any given situation. Users of this Standard should consult with the appropriate authorities having jurisdiction.

Users of this Standard should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgment should be used in employing the information contained herein.

All rights reserved. No part of this work may be reproduced, translated, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 1220 L Street, NW, Washington, DC 20005.

Copyright © 2014 American Petroleum Institute

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.

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

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

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, 1220 L Street, NW, Washington, DC 20005. 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, 1220 L Street, NW, Washington, DC 20005.

Suggested revisions are invited and should be submitted to the Standards Department, API, 1220 L Street, NW, Washington, DC 20005, standards@api.org.

Contents

Contents

Standard for Subsea High Integrity Pressure Protection Systems (HIPPS)

1 Scope

This standard addresses the requirements for the use of high integrity pressure protection systems (HIPPS) for subsea applications. API 14C, IEC 61508, and IEC 61511 specify the requirements for onshore, topsides, and subsea safety instrumented systems (SIS) and are applicable to HIPPS, which are designed to autonomously isolate downstream facilities from overpressure situations. This document integrates these requirements in order to address the specific needs of subsea production. These requirements cover the HIPPS pressure sensors, logic solver, shutdown valves, and ancillary devices including testing, communications, and monitoring subsystems.

2 Normative References

The following referenced documents are 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.

API Specification 6A, *Specification for Wellhead and Christmas Tree Equipment*

API Recommended Practice 6HT, *Heat Treatment and Testing of Large Cross Section and Critical Section Components*

API Recommended Practice 17A, *Design and Operation of Subsea Production Systems—General Requirements and Recommendations*

API Specification 17D, *Subsea Wellhead and Christmas Tree Equipment*

API Specification 17E, *Specification for Subsea Umbilicals*

API Standard 17F, *Standard for Subsea Production Control Systems*

API Recommended Practice 17H, *Remotely Operated Tools and Interfaces on Subsea Production Systems*

API Recommended Practice 17P, *Recommended Practice for Design and Operation of Subsea Production Systems—Subsea Structures and Manifolds*

ANSI/ASME B31.3 [1, 2], *Process Piping*

ANSI/ASME B31.8, *Gas Transmission and Distribution Piping Systems*

AWS D1.1 [3], *Structural Welding Code—Steel*

IEC 61508, Parts 1 to 4 [4], *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511, Part 1, *Functional safety—Safety instrumented systems for the process industry sector*

---

1 American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, New York 10036, www.ansi.org.

2 ASME International, 2 Park Avenue, New York, New York 10016-5990, www.asme.org.

3 American Welding Society, 8669 NW 36 Street, #130, Miami, Florida 33166-6672, www.aws.org.

4 International Electrotechnical Commission, 3, rue de Varembé, P.O. Box 131, CH-1211, Geneva 20, Switzerland, www.iec.ch.

NACE MR 0175, *Petroleum and natural gas industries—Materials for use in H_2S-containing environments in oil and gas production*

ANSI/SAE J343 [5], *Test and Test Procedures for SAE 100R Series Hydraulic Hose and Hose Assemblies*

ANSI/SAE J517, *Hydraulic Hose*

SAE AS 4059, *Aerospace Fluid Power—Cleanliness Classification for Hydraulic Fluids*

3 Terms, Definitions, and Acronyms

3.1 Terms and Definitions

For the purposes of this document, the following definitions apply. Where applicable, these definitions are aligned with those found in the latest edition of IEC 61508-4.

3.1.1
alternative pressure source
Injection fluid used for a valve seal test that does not exceed the RWP of the HIPPS at its depth rating.

NOTE Injection fluid can be any fluid that can be introduced into the system not only for testing but also for flushing or preventing hydrates from forming.

3.1.2
beta factor (β)
Factor used to represent the proportion of the dangerous failure rate of a nonredundant subsystem that would occur due to common cause hardware failures, if a redundant configuration is adopted.

3.1.3
commissioning
Functional verification of equipment and facilities prior to initiating operations.

3.1.4
dangerous failure
Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the safety function operates correctly when required.

3.1.5
final element
Part of a SIS which implements the physical action necessary to achieve a safe state.

NOTE The final element includes HIPPS closure devices (isolation valves), control valves (used to apply or relieve hydraulic control fluid pressure which actuates the HIPPS closure device), and quick exhaust valves.

3.1.6
fortified section
Piping and equipment with an intermediate pressure rating somewhere between the SIP (high) and MAWP (low) ratings.

[5] SAE International (formerly the Society of Automotive Engineers), 400 Commonwealth Drive, Warrendale, Pennsylvania 15096-0001, www.sae.org.

3.1.7
hardware fault tolerance
HFT
Ability of a functional unit to continue to perform a required function in the presence of faults or errors.

NOTE In determining the HFT, no account is taken of other measures that may control the effects of faults such as diagnostics, and where one fault directly leads to the occurrence of one or more subsequent faults; these are considered as a single fault.

3.1.8
high integrity pressure protection system
HIPPS
Mechanical and electrical-hydraulic SIS used to protect production assets from high-pressure upsets.

3.1.9
logic solver
In relation to a HIPPS, a Logic Solver is defined as the portion of an SIS that performs one or more logic function(s) related to the safety function(s).

3.1.10
maximum allowable working pressure
MAWP
The highest operating pressure allowable at any point in any component other than a flowline during normal operation or static conditions.

3.1.11
operating pressure
Pressure in the equipment when the plant operates at steady state condition, subject to normal variation in operating parameters.

3.1.12
overpressure source
One or a combination of sources which can create a pressure buildup beyond the RWP of hardware downstream.

NOTE Examples include the reservoir, pressure or boosting equipment (i.e. pump/compressor), manifolds, or other fluid injection sources.

3.1.13
pipeline
Piping, risers, and appurtenances installed for transporting oil, gas, sulfur, and produced waters.

3.1.14
process hazard
Process upset that could result in loss of life, injury to personnel, pollution, or damage to production assets such as overpressure and the subsequent rupture or failure of the process equipment.

3.1.15
process safety time
The time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed.

3.1.16
rated working pressure
RWP
Maximum internal pressure that the equipment is designed to contain and/or control.

3.1.17
reliability
Likelihood of a given piece of safety-related equipment to remain in operation for the expected duration.

3.1.18
risk analysis
Determination of the frequency of the event (e.g. overpressure) and the ability of safeguards (e.g. HIPPS) to reduce the frequency or the consequence such that the event becomes tolerable, either by being very rare (unlikely) or by lessening the impact.

3.1.19
safe failure
Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

3.1.20
safe failure fraction
SFF
Property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.

NOTE Refer to the latest edition of IEC 61508 for additional information.

3.1.21
safety instrumented function
SIF
Safety function with a specified SIL which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

3.1.22
safety instrumented system
SIS
Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s) (for example, refer to Figure 1).

NOTE This can include either safety instrumented control functions or safety instrumented protection functions or both.

3.1.23
safety integrity level
SIL
Discrete level (one out of four) for specifying the safety integrity requirements of the SIFs to be allocated to the SIS.

NOTE SIL 4 has the highest level of safety integrity; SIL 1 has the lowest level.

3.1.24
shut-in pressure
SIP
Full internal product process pressure that is contained by the HIPPS at the seabed when the high-pressure source is abruptly isolated to protect lower pressure hardware downstream of the spec break.

3.1.25
specification (spec) break
Point at which equipment pressure rating changes from one RWP rating to a lower one (or vice versa) downstream.

NOTE These locations are defined by the normal operating conditions of a flow stream that allows the use of lower design pressure equipment.

3.1.26
subsea tieback
An offshore field developed with one or more wells completed on the seafloor, using subsea trees.

NOTE The wells are connected by flowlines and umbilicals (the pathways for electrical and hydraulic signals) to a production facility in another area.

3.1.27
systems integration test
SIT
A process conducted on land to verify the fit, form, and function between interfaces of all subsea equipment and associated running tools prior to offshore installation.

3.1.28
systematic failure
Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors.

3.1.29
validation
Validation within this document has the meaning of “type approval” and is the process of proving a design by testing to demonstrate conformity of the product to design requirements.

3.1.30
verification
All activities necessary to confirm that the installed and mechanically completed HIPPS and its associated instrumented functions, meets the requirements stated in the SRS.

3.2 Acronyms, Abbreviations, and Symbols

β	beta factor
χ^2	uncertainty of the reliability estimate
λ	failure rate
λD	dangerous failures
λDD	dangerous detected failures
λ_{du}	dangerous undetectable failures
λ_{TOT}	total failure rate
AA	AA trim
ANSI	American National Standards Institute
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
ASNT	American Society for Nondestructive Testing
AWS	American Welding Society

BSDV	boarding shutdown valve
CFR	Code of Federal Regulations
DC	diagnostic coverage
DCS	distributed control system
DCV	directional control valve
DNV	Det Norsk Veritas
DOT	Department of Transportation
EPU	electrical power unit
ESD	emergency shutdown
EUC	equipment under control
FAT	factory acceptance test
FIV	flowline isolation valve
FMECA	failure mode effects and criticality analysis
GOR	gas-oil-ratio
HBN	Brinnel hardness
HFT	hardware fault tolerance
HH	HH trim
HIPPS	high integrity pressure protection system
HPU	hydraulic power unit
HSCM	HIPPS subsea control module
IEC	International Electrical Commission
ISA	International Society of Automation
LOPA	layer of protection analysis
MAWP	maximum allowable working pressure
MCS	master control station
MOC	management of change
MTBF	mean time between failure
MTTF	mean time to failure
MTTR	mean time to repair
MWP	maximum working pressure
NACE	National Association of Corrosion Engineers
NDE	normally de-energized
NE	normally energized
OLF	recommended guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities of the Norwegian Continental Shelf
PCS	production control system
PE	programmable electronics
PES	programmable electronic system

PFD	probability of failure on demand
PLEM	pipeline end manifold
PLET	pipeline end termination
PR	performance requirement
PSD	production shutdown
PSH	pressure switch high
PSL	product specification level
PST	partial stroke testing
PSV	process safety valve
PT	pressure transmitter
QEV	quick exhaust valve
QRA	quantitative risk analysis
QTC	qualification test coupon
ROT	remotely operated tool
ROV	remotely operated vehicle
RP	recommended practice
RWP	rated working pressure
SAE	Society of Automotive Engineers
SAFE	safety analysis function evaluation
SCM	subsea control module
SCSSV	surface controlled subsurface safety valve
SDV	shutdown valve (isolation valve)
SEM	subsea electronics module
SFF	safe failure fraction
SIF	safety instrumented function
SIL	safety integrity level
SIP	shut-in pressure
SIS	safety instrumented system
SIT	systems integration test
SOV	solenoid valve
SRS	safety requirement specification
SWL	safe working load
UPS	uninterruptible power supply
USV	underwater safety valve
XZV	trip valve

4 System Considerations

4.1 Introduction and Overview

This section covers system elements that shall be considered when designing a HIPPS. HIPPS is an SIS used to protect downstream facilities and personnel, and prevent environmental release by containing high-pressure excursions.

The design and performance of the HIPPS, including all lifecycle activities, should be based on IEC 61511. Hazard and risk assessments shall be conducted to determine requirements for risk reductions, allocate safety integrity level (SIL) of the HIPPS, and demonstrate that the risk of overpressure has been adequately mitigated. Appropriate regulatory agencies should be consulted for additional design and operating requirements.

A typical HIPPS is shown in Figure 1.

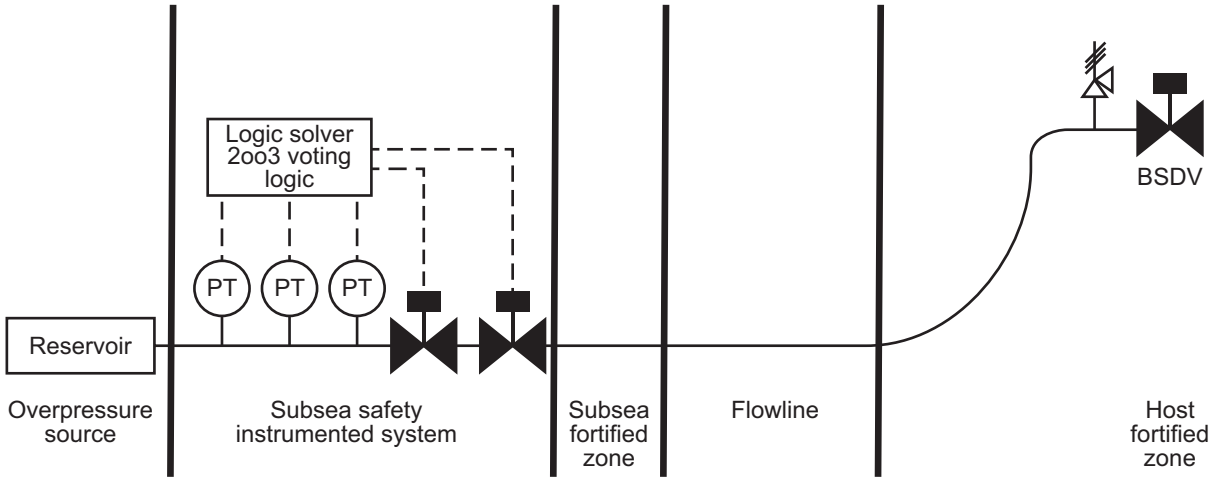

Figure 1—Typical Subsea Production HIPPS Valve Diagram

4.1.1 Pressure Source

The overpressure to be mitigated by the HIPPS could originate from a number of sources. Examples include, but are not limited to, high reservoir pressures, subsea booster pumps, connection to higher pressure pipelines, or a combination of these sources.

The source could be gas, liquid, or multiphase fluid, which have different system response requirements. The flow composition may change during the production life and may be dependent on topography. All of these aspects, and any uncertainties associated with them, need to be considered as part of a full HIPPS analysis. Before additional wells are tied into an existing system or any other change is made that could affect fluid properties, a new flow analysis shall be conducted to ensure that the system is designed to cover the new configuration.

4.1.2 HIPPS

HIPPS is an SIS, defined by this document, which provides pressure protection to downstream components.

4.1.3 Subsea Fortified Zone

A fortified section may be located downstream of the HIPPS isolation valves to allow time to respond to the system closure determined by the pressure transient calculations. The response time to system closure is dependent on the nature of the flow for the specific system and would include consideration of the gas-oil-ratio (GOR).

The pressure rating of the fortified section is project-specific and ranges from the maximum allowable working pressure (MAWP) of the flowline/pipeline, to the same as the full rating of the pressure source (e.g. subsea tree).

The length of the “fortified” section should be determined based on a transient flow analysis. The use of alternative flow assurance methods should not be included when determining the length of the fortified section. It is conceivable that this section may not be required, but this shall be proven based on flow analysis.

4.1.4 Unfortified Zone (Flowline)

The unfortified zone is downstream of the fortified zone and upstream of the host zone. The location of the unfortified zone shall be determined by the hydraulic analysis and be dependent on the impact of any eventual leakage risks to be mitigated. The hydraulic analysis should include all potential system transients (multiphase/slug flow, etc.). The unfortified zone shall be located to minimize risk of injury to people and damage to infrastructure and the environment. Design should also take into account the need for system testing.

The unfortified zone shall be proven to function by hydraulic analysis, design, and testing as appropriate.

4.1.5 Host Fortified Zone

The near-platform riser section shall be designed such that release of hydrocarbon or hazardous materials occurs away from the facility to protect personnel. Near-platform riser section refers to a region, which if breached by high-pressure excursions, could result in damage to the facility or threat to life.

4.1.6 Topsides

A process safety valve (PSV) upstream of the boarding shutdown valve (BSDV) can be used to relieve buildup of pressure due to valve leakage. Consideration needs to be given to safe venting of the PSV exhaust fluid.

4.2 Production Characteristics

Design of all product-containing systems shall consider the fluid and gas properties being transported and select materials and welding processes fully compatible with planned products.

For multiphase production systems, the full range of GOR, water production rates, sand, carbon dioxide, hydrogen sulfide, injected chemicals, and other products shall be fully investigated during analysis and design.

4.3 Flowline Rupture Considerations

Design of the flowline downstream of a HIPPS shall consider the possibility of failure of the HIPPS to correctly function. The design shall determine the likely consequences and design mitigations to minimize each consequence. Some of the key consequences of failure of the HIPPS and possible mitigations to consider include the following.

— Uncontrolled—In this case, the flowline ruptures and inventory is released to the environment. The system shall be arranged so that any pipeline burst occurs within the protective segment. Protection of human life is the highest priority. An environmental remediation plan should be in place.

— Controlled but Uncontained—In this case, there is a pressure-relieving mechanism which minimizes the quantity of product released. An environmental remediation plan should be in place.

— Controlled and Contained—In this case, there is a pressure-relieving mechanism (preferably self-resetting) which contains the release. The capacity of the containment system shall be defined.

4.4 Process Hazard and Risk Analysis

The decision to utilize a HIPPS shall be based on a qualitative and quantitative risk analysis (QRA) carried out in accordance with industry standards. Risk analysis requires determining the frequency of the event (overpressure) and the ability of safeguards (HIPPS, etc.) to reduce the consequences, such that the probability of the event becomes tolerable.

A qualitative risk analysis such as process hazard analysis shall be conducted using a defined methodology. The process hazard is typically overpressure and the subsequent failure of downstream equipment, potentially resulting in a loss of hydrocarbon containment. The risk is the frequency, or possibility of, overpressuring the equipment and the resulting consequences of equipment failure.

Quantitative analysis shall be performed [e.g. layer of protection analysis (LOPA)] as defined in IEC 61511. Risk thresholds shall be those mandated by the regulatory agency or the owner, whichever is the most stringent.

4.5 Selection and Determination of SIL

SIL is a representation of the required safety unavailability [average probability of failure on demand (PFD)] of a safety instrumented function (SIF). The SIL is expressed as a Level 1 through Level 4, which corresponds with Table 1.

SILs are determined, either in a prescriptive manner where a preselected SIL may be used when the application meets the required criteria, or a quantitative manner where the required SIL is calculated based on the risk thresholds, initiating frequencies, and other layers of protection to determine the required SIL of the HIPPS.

Table 1—SILs

SIL	PFD	Risk Reduction Factor
SIL 1	0.1 to 0.01	10 to 100
SIL 2	0.01 to 0.001	100 to 1000
SIL 3	0.001 to 0.0001	1000 to 10,000
SIL 4 [a]	0.0001 to 0.00001	10,000 to 100,000

[a] Not applicable in the process industry.

Determination of the HIPPS SIL should consider additional safeguards that are installed:

— pressure switch high (PSH) at facility, upstream of BSDV;

— PSH at each individual pressure source, upstream of HIPPS;

— PSV at facility upstream of the BSDV sized for either leakage rate (partial protection) or full flow rate; and

— reinforced section at facility riser.

SIL analysis is primarily conducted for safety; however, additional consideration may be for environmental or economic impacts. Additional safeguards (levels of protection) compliant with API 14C should be specified by the end user, and reflected in the end user's LOPA allocation and SIL requirement. The consideration with the highest SIL requirement may be used as the design basis.

4.6 Safety Requirement Specification (SRS)

4.6.1 General

The SRS is the controlling document for design, verification, and validation of the HIPPS in accordance with the project requirements and specifications and the basis for HIPPS performance monitoring and follow-up during the operating lifetime. The safety requirements specification shall meet the requirements of IEC 61511.

The SRS shall be kept current through management of change (MOC) process from concept development until the HIPPS is decommissioned.

The SRS shall include the following information or make references thereto:

— process description (which includes pressure ratings for all flowline segments) and summary of the documented hazard scenarios generated from the hazard analysis process;

— descriptions of functions performed by the SIF (in relationship to the associated hazard scenario) stating the functional relationship between process inputs and outputs including logic, mathematical functions, and any required permissives;

— SIL and PFD for each SIF;

— HIPPS process measurements together with their normal operating ranges and applicable trip set point tolerance;

— safe state of the process for each identified SIF, the sources of demand, and the demand rate;

— response time requirements for the HIPPS to bring the process to safe state;

— requirements for resetting the HIPPS after a trip;

— requirements for de-energize to trip;

— requirements for overrides/inhibits/bypasses/manual shutdowns, including how they are to be cleared;

— considerations for process common cause failures such as corrosion, plugging, power supply, etc.;

— actions to be taken in event of diagnosed dangerous failures;

— requirements for special start-up and HIPPS restart considerations;

— interface to other safety and process control systems;

— requirements for proof testing;

— desired testing frequencies, PFD, and mean time to failure spurious (MTTF spurious); and

— any additional information as required by the specific design.

4.6.2 HIPPS SIS

The HIPPS SIS shall be an autonomous safety system with a local logic system controlling HIPPS operation and shall include the following elements:

— multiple independent pressure sensing devices responding to the system pressure;

— high integrity logic processing subsystem;

— redundant final elements;

— HIPPS system reset to prevent automatic reopening of the HIPPS valves after a trip; and

— communications and additional equipment required for monitoring and testing the system.

HIPPS SIS subassemblies or components should be optimized for retrievability to support maintenance and availability requirements.

5 Design

5.1 Design Basis Requirements

5.1.1 Shut-in Pressure (SIP)

SIP is the full internal pressure that shall be contained by the HIPPS and upstream piping when the HIPPS has closed and all other upstream valves are open to the pressure source. Both transient pressure wave (water hammer effect) and sustained SIPs shall be quantified through a qualified and rigorous flow analysis using appropriate software tools. The flow analysis shall have access to information sufficient to model the production gas and fluid stream, reservoir, completion, production tubing, tree, flowline, riser, jumper, manifold, and HIPPS, as applicable. SIP should be determined for all life stages of the field production.

5.1.2 Fluid Properties

HIPPS shall be suitable for the GOR over the life of the HIPPS system and corrosive properties and compositions of the fluids. All components exposed to process fluids shall be designed in consideration of the expected corrosive properties. Temperatures of the process fluids during the operating life of the HIPPS and changing flow rates shall also be considered.

5.1.3 Upstream/Downstream Conditions

The upstream pressure rating, MAWP, and pipe size shall be determined outside of the HIPPS design. The final downstream pressure ratings, MAWPs, and pipe sizes shall be defined to meet the requirements of applicable specifications and additional requirements of this document. From this definition, the requirements of the HIPPS is provided to the HIPPS equipment designer/manufacturer.

5.1.4 Transient Pressure Due to Blockages

The possibility of abrupt blockage of the flowline at various points downstream of the HIPPS shall be considered. Calculations of the transient pressure increase arising from the blockages should be developed. Transient pressure calculations provide key guidance to designers on the minimum shut-in time necessary for the HIPPS to avoid overpressure of the flowline between the blockage and the HIPPS. It is essential that personnel with experience and knowledge scrutinize and validate transient pressure calculations.

To achieve this, the sum of the diagnostic test interval and the reaction time to achieve a safe state should be less than the “process safety time”. The process safety time is defined as the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed.

5.1.5 Reinforced Flowline Downstream of HIPPS (Fortified Section)

Blockages may occur near the HIPPS location. In this case, the resultant transient pressure rise may be very rapid and result in high pressures before the HIPPS valves achieve closure. Consequently, it may be necessary to increase the pressure rating or fortify the downstream flowline sections near the HIPPS. HIPPS valve closure time, set points for HIPPS closure, MAWP, and fluid characteristics (excluding additional flow assurance methods) shall all be carefully considered to determine length and pressure rating of the fortified section.

5.1.6 Flow Assurance

The potential for sudden blockages may be viewed as unlikely due to fluid properties and research into the specific fluids. This could be used to determine that a reinforced section is not required excluding alternative flow assurance methods, such as methanol injection.

5.1.7 Environmental Data

Environmental conditions are the site specific conditions that affect the design of the equipment, piping, and structures. Relevant information shall be supplied to the designer by the owner/operator. Detailed information on the site conditions shall be available to facilitate design of the HIPPS and piping components. The following list provides the typical information requirements. The list may need to be expanded depending on site conditions.

— Seabed pressure (water depth).

— Seabed Currents—Tidal, eddy, hurricane, tsunami, and other current information (current statistical specifications such as one-year return period and 100-year return period information).

— Seabed Temperatures—Expected average, maximum, and minimum seabed temperatures.

— Seabed Soils—Detailed characteristics of the soils and appropriate engineering properties of the soils.

— Seawater—Seawater information affecting the design of the facilities, such as density, salinity, H_2S content, or other.

— Site Depth—Local bathymetry of the site.

— Site Hazards—Specific site hazards should be investigated and considered (e.g. seabed slope, tsunami, earthquake, slope instability, and turbidity currents).

— Flowline axial movements due to thermal expansion loads.

5.1.8 Operational Requirements

The logic solver in the HIPPS module shall not permit bypassing of the HIPPS function. The logic solver may allow for changing a HIPPS trip set point according to approved procedures and subsequent testing, if permitted by regulatory requirement.

The HIPPS may be deactivated by mechanically locking open the valves via remotely operated vehicle (ROV) overrides, but bypassing of the HIPPS logic solver via the control system shall not be permitted, to minimize operator errors which could prevent the HIPPS from carrying out its assigned function. When a HIPPS valve is overridden by an ROV, appropriate safety steps shall be applied topsides to ensure operators are aware. HIPPS final element valves may only be fully locked open once operating conditions are reduced to a point where the SIS is no longer required.

5.1.9 HIPPS In-place Testing

Appropriate design of a HIPPS shall provide for regular testing to demonstrate correct functions of the HIPPS and monitoring of HIPPS operating status. The test interval shall be consistent with the basis of the SIL analysis. Design should allow for the following testing as determined by the SIL analysis.

— Regular Pressure/Leak Integrity Testing—The HIPPS shall be capable of demonstrating that the system has sufficient integrity to contain SIP with leakage less than the maximum leak rate. Testing interval is determined by SIL rating or regulatory requirement.

— Maximum Leak Rate Testing—The HIPPS design shall include appropriate methods to measure or infer the leak rate of the HIPPS for comparison to the predetermined maximum leak rate. Maximum leak rate determination shall consider both short-term shutdown events and long-term shutdown events such as a storm shut-in and shall either be set by the operator or by regulatory requirement.

— Pressure Sensors—Means shall be provided to reference a minimum of one pressure sensor against a known source. For example, this source can be a topsides source with the pressure adjusted for the installed depth and density of the fluid connecting the sensors. The “checked” sensor are then compared with all other HIPPS pressure sensors during operation to confirm that sensors are operating properly.

— Partial Stroke Testing (PST) of HIPPS Valves—For valves, partial operation with feedback on movement ~~can~~ may be applied when SIL requirements dictate a periodic testing interval more frequent than planned full closure testing intervals. PST shall be treated as a functional test which covers only a fraction of the possible failures and not as a self-test with diagnostic coverage. The fraction of possible failures shall be properly documented through a FMECA or fault tree analysis.

— Full Closure Testing—Full end-to-end testing shall be demonstrated from the HIPPS sensor trigger point to full closure of the HIPPS valves and any bypass valves that may be required to close.

5.1.10 HIPPS In-place Control and Diagnostic Function

The following data should be available at a minimum:

— Pressure Sensor Output—Pressure sensor measurements shall be supplied to the master control station (MCS) and to the HIPPS logic solver.

— HIPPS Isolation Valve Status—Inferred or directly measured valve status shall be supplied to the MCS. Inference shall not be based upon the commanded position, but through measurement of the actuator power supplied to the actuator.

— Tripped, voting, and alarm status shall be supplied to the MCS.

— Trip is a latched function requiring operator reset to clear. The operator shall have the means to reset the HIPPS trip logic and command the barrier valves to open/close only when acceptable local pressures exist at the HIPPS sensors and reset is allowed by the logic solver. The operator shall not have trip reset capability if the local pressure at the HIPPS sensors is above the trip pressure.

— HIPPS Controller Status Report—The HIPPS local controller shall have self-diagnostic functions and reporting of the controller status to the production control system.

5.1.11 Sharing of HIPPS Valves

HIPPS systems may share valves with the production control system (PCS) based on the following restrictions.

— PCS and HIPPS shall use separate solenoids/pilots to actuate the same valve, both solenoids shall be engaged and held on for the valve to open. Nothing shall prevent the HIPPS solenoid from closing the actuated valve. If other technology is used, the same philosophy shall apply.

— Designated underwater safety valve (USV) and surface controlled subsurface safety valves (SCSSVs) may not be shared.

NOTE No credit for the PCS can be taken in the risk analysis if the valves are shared with the HIPPS.

5.1.12 Operating Cycles

Product designs shall be capable of performing and operating in-service as intended for the number of operating cycles as specified by the manufacturer. Number of operating cycles should be at least 10 times the number of planned closure tests required for the SIL rating.

5.1.13 Pigging Considerations

HIPPS components may require pigging capability. A pigging analysis should be completed to ensure that the system is not damaged during the pigging operation. The analysis should consider the possibility of plugging of sensors and small bore piping connections.

5.1.14 Venting

The design shall consider the venting of trapped pressure and ensure that trapped pressure can be safely released prior to the disconnection of fittings, assemblies, etc.

5.1.15 Sand

The requirements for valves to be rated for standard or sandy service, as determined by API 6A and tested, per API 6AV1, should be clearly defined by the end user.

5.1.16 Intervention

ROV interventions and their respective functions shall conform to API 17H.

5.2 Modes of Failure

5.2.1 Electrical Power

The electrical power system shall be designed in accordance with API 17F. Failure of the electrical power (either completely or due to reduced voltage) shall cause the isolation valves to close.

5.2.2 Communications Systems

Failure of the communication system shall not prevent the HIPPS logic controller from carrying out its required functions. An operational procedure shall address the necessity (or not) for the operator to activate the HIPPS function by means of shutting down the electric or hydraulic power.

5.2.3 Actuator Power

Actuator power shall be used only to open the closed valve. The actuator shall be designed to work in fail-close manner (from a HIPPS logic solver command or actuator power failure); utilizing valve bore pressure, and/or spring force to assist closing the valve. The closing force shall be sufficient to fully close the valve when the internal pressure reaches or exceeds the HIPPS triggered pressure.

The Hydraulic supply system shall be designed in accordance with API 17F. Failure of the hydraulic supply shall cause the isolation valves to close.

5.3 Temperature

5.3.1 General

The requirements for all HIPPS equipment shall be clearly defined by the end user. Temperature rating data of the HIPPS shall be based on the process conditions, environmental conditions, and conditions during testing and installation. Consideration shall be given to components that, under certain conditions, may generate heat and impact the overall system temperature.

5.3.2 Temperature Ratings

The requirements for valves to be rated for temperature class, as determined by API 17D shall be clearly defined by the end user. Consideration should be given to equipment operation (tested) in “cold weather” environments and transitional low-temperature effects on associated downstream components when subject to Joule-Thomson cooling effects due to gas pressure differentials.

5.4 Pressure

5.4.1 General

The definition of pressure rating shall consider the effects of transient flow, pressure containment, and other pressure induced loads. The effects of hyperbaric loads shall also be considered.

a) Hydraulic Control Component—Hydraulic control component should be specified by the manufacturer, per API 17F for working, design, and test pressures.

b) External Hydrostatic Pressure—Loading due to the external hydrostatic pressure shall be considered.

c) Rated working pressure (RWP) of HIPPS isolation and ancillary valves should be specified by the end user, based on the MAWP and SIP.

5.4.2 Pressure Ratings

5.4.2.1 General

The pressure rating shall be based on the maximum pressure that the system sees at any time during its field life and should be specified by the end user. In addition, the effects of external loads (i.e. bending moments, tension), ambient hydrostatic loads, and fatigue shall be considered.

5.4.2.2 RWP

Whenever possible, assembled equipment that comprises pressure-containing and pressure-controlling portions of HIPPS equipment, such as valves, connections, tees, and crosses, shall be specified by the end user per API 17D. Piping and plumbing associated with HIPPS sensors, flow bypasses, chemical injection, hydraulics, etc. shall conform to the RWP requirements of API 17D.

5.4.2.3 Nonstandard Pressure Ratings

All other piping exterior to the HIPPS equipment should conform to the design requirements and piping codes specified by the end user. This requirement applies to portions of a protected system, such as manifolds, pipelines, pipeline end terminations (PLETs), and pipeline end manifolds (PLEMs). These systems shall be designed to MAWP and fortified section requirements. For more information, refer to API 17P.

5.4.3 Alternative Pressure Source

All alternative pressure sources, such as injection fluid used for valve seal test and for calibrating the pressure sensors and proof testing the HIPPS, shall not exceed the MAWP or RWP of the HIPPS equipment.

5.5 Control System Design

5.5.1 General

The HIPPS control system (known as logic solver in IEC 61511) shall be independent from the PCS. The HSCM components may be packaged with the PCS subsea control module (SCM) and share electrical power and hydraulic supply, if practical.

No HIPPS overriding commands may be allowed. Trips are a latched function requiring operator reset to clear. The operator shall have the means to reset the HIPPS trip logic and command the barrier valves to open/close only when acceptable local pressures exist at the HIPPS sensors and reset is allowed by the logic solver. The operator cannot have trip reset capability if the local pressure at the HIPPS sensors is above the trip pressure.

The HIPPS controller shall have self-diagnostic functions and reporting of the controller status and sensor data made available to the topside MCS. Diagnosed critical dangerous failures of the HIPPS control system shall close the HIPPS valves after triggering a production shutdown (PSD) via the PCS.

5.5.2 HIPPS Set Point

The HIPPS trip pressure set point shall meet the requirements of the system design with respect to over pressure protection and cannot be changed by the control room operator. The system design shall inhibit the operator from making changes that could override or alter the autonomous operation of the HIPPS logic solver or system.

5.5.3 Actuation of HIPPS Isolation Valves

The means and hydraulic pressures which the control system utilizes to open the HIPPS isolation valve shall be specified by the manufacturer, per API 17D, for the SIP, MAWP, and trip set pressure values provided by the end user.

5.5.4 Communication

The protocol selected for use in subsea control communications shall be based on the applicable industry standards set forth in API 17F. System design shall allow for noise, crosstalk, and other disturbances in the operating environment without malfunction.

5.5.5 Process Equipment Design Basis

The process components of the HIPPS include all equipment that is subjected directly to the internal pressures, external pressures, and internal and external temperatures during their service life. Examples of such equipment are isolation valves, piping, injection valves, flanges, tees, and crosses. Connection bolting shall be considered as a part of the pressure isolation component’s end flange.

5.5.6 SIL Compliance

The physical component architecture of the HIPPS SIF shall meet the following requirements:

a) the SIL shall meet or exceed the specified SIL and this requirement shall be demonstrated by analysis per IEC 61508 and IEC 61511;

b) the system shall be shown to comply with low demand mode operation; and

c) the architectural constraints shall comply with the minimum hardware fault tolerance (HFT) as specified in IEC 61511. Alternative fault tolerance requirements from IEC 61508 may be used providing an assessment is made.

5.6 Materials Class Rating

Material class of HIPPS equipment exposed to wellbore fluids shall be specified by the end user, per API 17D requirements.

5.7 External Hydrostatic Pressure

External hydrostatic pressure may be considered in the design of HIPPS equipment hardware, per API 17D guidelines. MAWP shall not exceed the RWPs of manufacturer specified HIPPS equipment, per API 17D, including the effects from fluid density creating a hydraulic head. External pressure effects are not allowed in the determination of MAWP conditions for a HIPPS SIS.

5.8 Transportation and Installation Conditions

Transport and installation conditions are specific load conditions that affect the design of the piping and structures and should be specified by the end user. Allowable design loads are included as a part of the manufacturers design documentation, per API 17D and made available to the end user for review. Detailed information on the transport and installation conditions is necessary to facilitate design of the HIPPS facilities and piping components.

The following list provides the typical information requirements; this list may need to be expanded depending on site conditions.

a) Transport Loads—Components shall be lifted and transported during fabrication, transportation, and installation. Appropriate design loads, connection interfaces, and conditions shall be supplied to the designers.

b) Installation Loads—HIPPS components shall be lowered to the seabed. Appropriate design loads, connection interfaces, and conditions shall be supplied to the designers. An engineering interface between the designers and installation contractors is necessary to assure correct conditions are considered.

5.9 Equipment Design

5.9.1 General Requirements

Design shall consider marine growth, fouling, corrosion, hydraulic operating fluid, and, if exposed, the well stream fluid.

5.9.2 Product Specification Levels (PSLs)

All pressure-containing and pressure-controlling parts of equipment manufactured shall conform to the requirements of PSL 3 or PSL 3G for gas service as established in API 17D.

5.9.3 Corrosion

External corrosion and its mitigation for HIPPS equipment shall conform to API 17D guidelines. Consideration should be given to the corrosion protection design for all piping external to the HIPPS system (pipelines, PLEMs, PLETs, jumpers, etc.) and how it may interact with the corrosion protection design specified by the manufacturer for the HIPPS equipment.

Corrosion protection and interaction based upon a marine environment shall consider, at a minimum, the following:

— external fluids;

— internal (bore) fluids;

— internal (hydraulic and test medium) fluids;

— weldability;

— crevice corrosion;

— dissimilar metals effects;

— cathodic protection effects; and

— coatings.

Corrosion resistant inlays of end connections shall be made in accordance with API 17D.

5.9.4 Erosion

The possibility of erosion in the flowline and HIPPS parts at points of flow direction changes shall be considered and mitigated during design.

5.10 Control Systems Components

5.10.1 HIPPS Subsea Control Module (HSCM)

The HSCM should satisfy the requirements given in IEC 61508, IEC 61511, and API 17F for hardware and software as applicable.

The HSCM contains the electrical/electronic and hydraulic control components. The major items include the subsea electronic module (SEM), electrohydraulic solenoid valves, hydraulic DCVs, accumulators, electrical connectors, and hydraulic couplers.

The HSCM components may be packaged with the PCS SCM and share electrical power and hydraulic supply. The HIPPS components shall remain functionally segregated, and failure of other packaged components shall not prevent HIPPS from carrying out its required functions. In the case where the HSCM and PCS actuate the same valves (e.g. christmas tree master valve), the HSCM should be packaged with the PCS SCM and share electrical power, hydraulic supply, and DCVs, provided the required PFD is met.

Retrievability should be a primary consideration in the design of the HSCM assembly.

5.10.2 SEM

The SEM primarily houses the control electronics (logic solver), power supplies, and communications circuits (modem).

The SEM enclosure should have at least two levels of integrity against water intrusion (such as multiple O-rings). The enclosure design should provide a means of testing the seals.

5.10.3 Logic Solver

The logic solver (controller) hardware shall be designed in accordance with IEC 61508. It is sometimes referred to as the “electronics trigger module.” The logic solver shall be certified as to its suitability for use at a certain SIL rating. The controller SIL rating shall be the same or better than the system application requirement.

The HIPPS controller logic shall provide for autonomous operation of the system. The logic functions shall include, but are not limited to, the following:

— monitor system pressure;

— alarm at High-pressure condition;

— perform majority voting logic of transmitter data;

— diagnose faulty transmitter;

— alarm and close HIPPS valve(s) at HIGH-HIGH-pressure condition and on diagnosed serious dangerous faults;

— report system fault diagnostics, status, and pressure data to the production control system;

— perform operator initiated test functions (e.g. partial valve closure testing);

— perform operator initiated reset function after HIGH-HIGH-pressure condition no longer exists;

— perform operator initiated valve closure or opening (if permitted); and

— diagnosed serious dangerous faults.

5.10.4 Sensors

These components should be considered as part of a critical sensor system. The sensor system design should attempt to minimize the complexity of the instrumentation and emphasize reliability and availability. The sensor design should satisfy all the physical, operational, and environmental requirements for the application.

The preferred sensing device for monitoring the produced fluid pressure is the pressure transmitter. Discrete switches shall not be used.

The selection process of the sensors should include reference to API 17F and IEC 61508.

Sensors selected for the HIPPS should be very high reliability types. Sensor system reliability and availability may be enhanced by redundancy. The sensors should have reliability data for use in the system SIL calculations. The number and placement of sensors is system design dependent with consideration given to high-pressure detection, testing, and start-up after HIPPS valve closure.

A sensor fault or failure shall not prevent the proper operation of the system.

Sensor positioning should minimize the potential for any hydrate blockage compromising sensor operation.

5.10.5 Control/Valve Interface

The control/valve interface typically consists of solenoid-operated DCVs and hydraulically-piloted DCVs to supply hydraulic fluid to the HIPPS isolation valves. Other technology may be used provided it meets all requirements for reliability and availability. The solenoid-operated DCVs and hydraulically-piloted DCVs shall have an RWP equal to or greater than the RWP of the hydraulic control system.

The control/valve interface shall be designed for fail-close operation of the HIPPS isolation valves. The solenoid-operated DCVs shall not be “latched” in the open position, but require electrical power to be maintained to keep them in the open position.

5.10.6 Topsides System

The topsides equipment typically consists of the MCS, hydraulic power unit (HPU), uninterruptible power supply (UPS), and electrical power unit (EPU). When used with the PCS, the HIPPS utilizes the required topsides equipment. The HIPPS ancillary and data gathering functions may be performed by a PCS. These elements may be integrated within the host facility distributed control system (DCS). The safety functions of the HIPPS shall not be integrated with the control functions of the PCS and DCS. The MCS also permits the operator to initiate various HIPPS test functions and reset the system after a high-pressure event has been rectified.

5.10.7 Umbilical Systems

The safety functions of the HIPPS shall operate as a stand-alone system from that of the PCS and the subsea umbilical. It is acceptable to integrate the HIPPS utility supplies (electrical, hydraulic, communications, and injection chemicals) within the umbilical. The umbilical should be designed in accordance with API 17E and umbilical jumpers should be designed in accordance with API 17F.

If the HIPPS is added for operation with a preexisting PCS, analysis is required for electrical power, communication signals, and hydraulics in order to verify proper operation with the added equipment. Alternatively, determine if changes are required, in order to verify that the HIPPS systems are not adversely impacted by normal operations by incorporating it within a preexisting PCS.

5.10.8 HIPPS Isolation Valves

The valves and actuators used in the HIPPS final element of a HIPPS SIS shall be designed and tested in accordance with the applicable sections of API 17D.

The valve fail-close function shall utilize valve bore pressure and/or actuator spring force to assist closing the valve. The closing force shall be sufficient to fully fail-close the valve when the flowline pressure reaches the HIPPS triggered pressure and the closing time shall be equal or less than the time required by the system analysis. The valve shall also be able to close when the internal bore pressure is at least equal to water depth ambient pressure and hydraulic pressure is lowered to 100 psi above the water depth ambient pressure.

The actuator shall be qualified to open the valve when under the maximum specified operating conditions defined by the design of the HIPPS system. The maximum valve opening pressure shall be suitable to allow a hydraulic system design in accordance to API 17D. Preferably, the maximum valve opening pressure should be 30 % below the nominal hydraulic operating pressure. The valve/actuator should have valve position indication sensors. These may be 0 % to 100 % valve position or full open/full close position indicators (limit switch, etc.); other means (hydraulic pressure/valve signature) may be used.

It is the end user’s responsibility to select the valve size based on pipe line flow bore diameter and pigging operation. If the API valve bore diameter is different than the pipe flow bore diameter, the design should minimize flow turbulence, and allow unfettered pig passage. Valves and valve blocks having flanged end connection shall use integral or studded outlets that conform to the requirements of API 17D.

Only threaded connections defined per API 17D are allowed. No internal threaded end connections (threads manufactured into the valve body) are allowed.

For units having end and outlet connections with different pressure ratings, the rating of lowest rated pressure containing part shall be the rating of the unit.

Loose threaded flanges and other threaded end and outlet connections shall not be used on HIPPS subsea equipment handling produced fluid. Threaded connections, such as instrument connections, test ports, and injection/monitor connections, may be used in sizes up to 25.4 mm (1.00 in.). If integral flange threaded connections are used, there shall be an isolation valve and either a bolted flange or a clamp hub connection on the HIPPS side of the threaded connection. Threaded connections shall conform to the requirements of API 17D. Threaded bleeder/grease/injection fittings shall be allowed without an isolation valve and flange/clamp hub if at least two pressure barriers between the produced fluid and the external environment are provided and the sealing area shall be made of corrosion-resistant materials.

Welded outlet hubs are acceptable; however, the design and manufacturing shall conform to the design stress and quality, material control specified by API 17D. The design should consider the external loading from piping, material differences, and cathodic protection schemes.

5.11 Factory Acceptance Testing (FAT)

Each subsea valve and valve actuator shall be subjected to a hydrostatic and operational test to demonstrate the structural integrity and proper assembly and operation of each completed valve and/or actuator, per API 17D for PSL 3 or PSL 3G for gas service, as specified by the end user.

5.12 SIL Evaluation

The SIL evaluation/rating of the HIPPS shall include reliability analysis of all fundamental components of the system. These typically are:

— sensors (pressure transmitters);

— logic solver;

— solenoid-operated control valves;

— DCVs; and

— valves/actuators.

Any component associated with HIPPS that could influence or prevent the HIPPS from performing its primary function shall be included in the SIL evaluation.

Reliability data for each component are required to perform the SIL evaluation and determine the overall system PFD.

5.13 Piping and Structures Specific Design Requirements

5.13.1 General

The subsea structure, piping and general design should be in accordance with API 17P.

5.13.2 Piping

ANSI/ASME B31.3 or ANSI/ASME B31.8 shall act as the primary reference on design of piping and pressure-rated components.

5.13.3 Structure

ANSI/ASME B31.3 or ANSI/ASME B31.8 shall act as the primary reference on design of piping structural support elements.

5.13.4 Piping Connections

Piping connections with the flowline or flowline jumper may encounter high loadings (bending and torsion) due to flowline axial movements and loading. Consideration of the effects of flowline movements on connector design is required.

5.13.5 End Flange and Outlet Connections

Tees, crosses, flanges, and hubs, or other end connections for subsea use shall be designed according to API 17D. Gasket selection and corrosion-resistant inlays of end connections shall be made in accordance with API 17D.

5.13.6 Closure Bolting

Closure bolting and makeup for HIPPS equipment shall be designed in accordance with API 17D.

6 Materials

6.1 HIPPS Final Element Equipment

6.1.1 General

The material performance, processing, and compositional requirements for all pressure-containing and pressure-controlling components associated with HIPPS final element devices should conform to API 6A.

6.1.2 Material Properties

In addition to the materials specified in API 6A, other higher strength materials may be used provided they satisfy the design requirements of API 6A and conform to the manufacturer’s written specifications. The impact values required by API 6A are minimum requirements and higher values may be specified to meet local legislation or user requirements.

For pressure-containing forged material, forging practices, heat treatment, and test coupon [qualification test coupon (QTC) or prolongation] requirements shall be in accordance with API 6HT with the additional requirement that the test coupon accompany the material it qualifies through all thermal processing.

6.1.3 Corrosion Considerations

HIPPS should be constructed with materials (metallic and nonmetallic) suitable for its respective material classification as described in API 17D. These specifications do not define all factors within the bore fluid environment, but do provide basic service conditions and relative corrosivity. Corrosion from marine environment should be considered.

6.1.4 Material Classes

It is the responsibility of the end user to specify materials of construction for pressure-containing and pressure-controlling components associated with HIPPS final element devices. Material Class AA through Class HH, as defined in API 17D, shall be used to indicate the material of those equipment components. Other bore pressure boundary penetration equipment, such as grease and bleeder fittings, shall be treated as “stems” as specified in API 6A. Metal seals shall be treated as pressure-controlling parts as specified in API 6A.

All pressure-containing components exposed to bore fluids shall be in accordance with API 17D materials, Class AA through Class HH.

6.1.5 Temperature Ratings

6.1.5.1 General

The following temperature conditions need to be considered.

6.1.5.2 Standard Operating Temperature Rating

Temperature classifications indicate temperature ranges, from minimum ambient to maximum flowing fluid temperatures. Classifications are defined in API 6A and API 17D. To meet impact toughness requirements, the minimum classification for pressure-containing and pressure-controlling materials should be temperature classification U, –18 °C (0 °F) to 121 °C (250 °F).

6.1.5.3 Standard Operating Temperature Rating Adjusted for Seawater Cooling

If the manufacturer shows through analysis or testing that certain component assemblies on subsea HIPPS equipment will not exceed specific allowable material temperatures while operated subsea with a retained fluid at the standard operating temperature, then this equipment may be designed and rated to operate at the standard operating temperature.

Conversely, subsea components and equipment which are thermally shielded from sea water by insulating materials shall demonstrate that they can work within the temperature range of the designated standard operating temperature classification.

6.1.5.4 Storage/Test Temperature Considerations

If subsea equipment is to be stored or tested on the surface at temperatures outside of its temperature rating, then the manufacturer should be contacted to determine if special storage or surface testing procedures are recommended. Manufacturers shall document any such special storage or surface testing considerations.

6.1.6 PSL

All material requirements for pressure-containing and pressure-controlling components of HIPPS closure devices shall conform to PSL 3 or PSL 3G for gas service as established in API 17D. These PSL designations define different levels of requirements for material qualification, testing, and documentation in accordance with API 6A and API 17D.

Base metal of pad eyes and other lifting devices should meet PSL 3 load bearing requirements of API 17D.

Structural components and other non-pressure-containing/controlling parts of equipment are not defined by PSL requirements but by the manufacturer’s specifications.

6.1.7 Closure Bolting

Selection of closure bolting materials and their coating/plating should consider seawater induced chloride stress corrosion cracking and corrosion fatigue. Some high strength bolting materials may not be suitable for service in a seawater environment. Closure bolting manufactured from carbon or alloy steel when used in submerged service shall be limited to 321 HBN (Rockwell “C” 35) maximum due to concerns with hydrogen embrittlement when connected to cathodic protection.

Closure bolting shall conform to PSL 3 requirements of API 17D. Closure bolting for material classes AA through HH that is covered by insulation shall be treated as exposed bolting per API 17D.

6.2 HIPPS Control System and Final Element-mounted Control Devices

6.2.1 Material Properties

It is the responsibility of the end user to specify materials of construction (metallic and nonmetallic) for HIPPS closure device-mounted control devices which come in contact with bore fluids. Material classes AA through HH as defined in API 17D shall be used to indicate the material of closure device mounted control devices. It does not define all factors within the bore fluid environment, but provides material classes for various levels of service conditions and relative corrosivity.

It is the responsibility of the manufacturer to specify materials of construction for all other components associated with the HIPPS control system, as recommended by API 17F. Other higher strength materials may be used provided they satisfy the design requirements of API 17F and conform to the manufacturer’s written specifications.

The manufacturer should be aware of the sea water environment and temperature from close proximity to closure and closure device-mounted devices and select materials accordingly. Subsea components and equipment which are thermally shielded from sea water by insulating materials shall demonstrate that they can work within the temperature range of the designated HIPPS closure device.

6.2.2 Material Classes and Temperature Ratings

Material class and temperature rating for devices which come in contact with bore fluids (i.e. sensors) shall be the same as designated for HIPPS closure devices.

Material class and temperature rating for other HIPPS control system devices should be specified in accordance with API 17F.

6.2.3 Corrosion Considerations

Pipe/tubing and end fittings, connectors, and connector plates shall be made of materials that withstand atmospheric and sea water corrosion. Pipe/tubing/hoses that contact bore fluids or injected chemical shall be made from materials compatible with those fluids.

6.2.4 Seal Materials

Seal materials shall be suitable for the type of hydraulic control fluid to be used in the system. Seals which contact bore fluids or injected chemicals shall be made of materials compatible with those fluids.

6.3 Welding

Welding of pressure-containing/controlling component, structural components and corrosion-resistant overlays shall conform to the requirement of API 6A, API 17A, and API 17P.

6.4 Coatings (External)

External corrosion control for HIPPS equipment should be provided by appropriate materials selection, coating systems, and cathodic protection. A corrosion control program is an ongoing activity which consists of testing, monitoring, and replacement of spent equipment. The implementation of a corrosion control program is beyond the scope of this standard.

The coating system and procedure used shall conform to the written specification of the equipment manufacturer, the coating manufacturer, or API 17D. Color selection for underwater visibility shall be in accordance with API 17A.

The manufacturer should maintain, and have available for review, documentation describing the coating systems and procedures used.

7 Quality Control

7.1 General

For this standard, HIPPS SIS components are subdivided into three categories to appropriately identify quality control requirements for specific hardware groups manufactured and assembled into a HIPPS, the categories are as follows.

— HIPPS Final Element Devices—Governed by PSL, as specified in API 17D.

— HIPPS Final Element-mounted Devices—Governed by API 17D, API 17F, and IEC 61511.

— HIPPS Control System Devices—Governed by PFD and HFT, as specified in IEC 61508 and IEC 61511.

For ancillary components not specifically covered by these categories, quality control requirements should conform to the manufacturer's written specifications.

Reference should also be made to the requirements of IEC 61508 and IEC 61511 for management of the safety lifecycle including planning, assigning responsibilities, competence of people to fulfill their responsibilities, validation (check that the outputs of each activity meet the expected outputs), and functional safety assessment.

7.2 HIPPS Closure Devices—PSL

7.2.1 General

Quality control and testing of pressure-containing and pressure-controlling components and assemblies of HIPPS closure devices, regardless of specified SIL, shall conform to requirements for PSL 3 or PSL 3G for gas service, as established in API 17D.

7.2.2 Hydrostatic Testing for HIPPS Closure Devices

Procedures for hydrostatic pressure testing of HIPPS closure devices shall conform to the requirements defined in API 17D for PSL 3.

7.2.3 Gas Testing for HIPPS Closure Devices

Procedures for Pressure Testing of HIPPS closure devices shall conform to the requirements for PSL 3G as described in API 17D.

7.2.4 Hydraulic System Pressure Testing

Components which contain hydraulic control fluid shall be tested to a hydrostatic body/shell test at 1.5 times hydraulic RWP or their respective hydraulic systems per API 17D, PSL 3. All operating subsystems (actuators, connectors,

etc.) that are operated by the hydraulic system should function at 0.9 times hydraulic RWP or less of their respective system pressure.

The hydraulic system does not communicate with the bore, therefore, its MWP and test pressure should be limited to the weakest pressure containing element or less, as specified by the manufacturer. The test medium is the hydraulic system fluid. Acceptance criteria should be no visible leakage as defined in API 17D.

7.2.5 Drift Test

Drift testing should be conducted per the manufacturer's written specifications. HIPPS closure devices with bore sizes per API 6A should be physically drifted using the API 6A specified drift mandrel. Runs that require passage of flowline/pipeline pigs should be physically drifted with the recommended drift mandrels associated with the pipeline pigs.

7.2.6 Pipe/Tubing/Hose

Allowable stresses in pipe/tubing should be in conformance to ANSI/ASME B31.3. Hose design shall conform to ANSI/SAE J517 and shall include validation to ANSI/SAE J343.

Testing of assembled pipe/tubing/hose and end fittings, connectors, and connector plates exposed to bore fluids and/or otherwise directly associated with the HIPPS closure device should conform to the requirements API 17D. The hydraulic system does not communicate with the bore of the HIPPS closure device, therefore, plumbing MWP and test pressure should be limited to the weakest pressure containing element or less, as specified by the manufacturer. The test medium is the hydraulic system fluid. Acceptance criteria should be no visible leakage, per API 17D. Chart recording is not required.

7.2.7 Optical Cables and Cable Penetrations

Optical fibers shall be routed inside fluid-filled conduits; typically, a fluid-filled hose for flying lead or short cable applications and a metal tube for longer umbilical applications. Optical terminations shall include qualified penetrations to prevent fluid leakage from these conduits. Optical penetrations into pressure containing cavities or piping systems shall be qualified for full differential pressure across the penetration. Optical fibers run in fluid-filled hoses shall include sufficient internal fiber slack length to prevent fiber tensioning under expected load conditions.

7.2.8 Routing

The routing of all pipe/tubing/hose/electric or optical cable shall be carefully planned, and it should be supported and protected to minimize damage during testing, installation/retrieval, and normal operation of the subsea system. Free spans shall be avoided and where necessary it shall be supported and/or protected by trays/covers. The bend radius of cold bent tubing shall not exceed the NACE MR 0175 requirements for cold working. Cold bend shall be in accordance with ANSI/ASME B31.3. Tubing running to hydraulic connectors should be accessible to divers/ROV/remotely operated tool (ROT) such that it can be disconnected, vented, or cut, to release locked in fluid and allow mechanical override

Electrical cables should be routed such that any water entering the compensated hoses moves away from the end terminations by gravity. Electrical signal cables should be screened/shielded to avoid crosstalk and other interferences.

7.2.9 Flushing

After assembly, all tubing runs and hydraulically-actuated equipment shall be flushed to meet the cleanliness requirements of SAE AS 4059. Class of cleanliness shall be as agreed between the manufacturer and purchaser. Final flushing operations shall use a hydraulic fluid compatible with the fluid to be used in the field operations. Equipment shall be supplied filled with hydraulic fluid. Fittings, hydraulic couplings, etc. shall be blanked off after completion of flushing/testing to prevent particle contamination during storage and retrieval.

7.3 Structural Components

Quality control and testing of welding for structural components should be as specified for non-pressure-containing welds as established in AWS D1.1. Weld locations where the loaded stress exceeds 50 % of the weld or base material yield strength, and welded pad eyes for lifting, are identified as “critical welds” and should meet PSL 3 quality control and testing requirements defined in API 6A.

7.4 Lifting Devices

Quality control requirements for pad eyes and lifting devices should meet quality control and testing requirements defined in API 17D.

7.5 Cathodic Protection

Electric continuity tests shall be performed to prove the effectiveness of the cathodic protection system. If the electrical continuity is not obtained, earth cabling shall be incorporated in the ineffective areas where the resistance is greater than 0.1 ohms.

7.6 Storing and Shipping

All equipment shall be drained and lubricated in accordance with the manufacturer's written specification after testing prior to storage or shipment. The manufacturer should provide recommendations concerning shipment, storage (including recommended environment), and maintenance requirements.

Prior to shipment, parts and equipment shall have exposed metallic surfaces (except those specially designated such as anodes or nameplates) either protected with a rust preventive coating or filled with a compatible fluid containing suitable corrosion inhibitors in accordance with the manufacturer’s written specification. All flange faces, clamp hubs, and threads should be protected by suitable covers. Equipment already coated, but showing damage after testing, should undergo coating repair prior to storage or shipment.

For shipment, units and assemblies should be securely crated or mounted on skids so as to prevent damage and to facilitate sling handling. Consideration should be given to transportation and handling onshore as well as offshore.

8 Equipment Marking

All subsea markings should conform to API 17H and API 17A.

9 Validation

9.1 General

NOTE The term ‘Validation’ as used in this section has a distinctly different meaning when compared with the definition used in IEC 61511 or ANSI/ISA 84.00.01. In this section, the term ‘Validation’ has the meaning of ‘Type Approval’ rather than the meaning given in the international standards: “The activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification” (IEC 61511-1 definition of Validation).

This section defines the validation requirements to be used to qualify the product designs of key components of the HIPPS and the overall HIPPS assembly formed by these key assemblies.

At a minimum, key HIPPS components shall include:

— sensors;

— logic solver;

— final element which includes:

  — control valves (used to apply or relieve hydraulic control fluid pressure which actuates the HIPPS closure device); quick exhaust valves (QEVs);

  — HIPPS closure devices (isolation valves).

— isolation or bypass valves used for pressure monitoring/bleed, chemical injection, etc.

Validation testing of key components may be performed individually. However, the final element assembly of a HIPPS should undergo additional testing not cumulative to other validation tests.

Validation should address more than the physical testing of a component. Validation should also include a review of any qualification testing as well as a review of the reliability/PFD calculations.

NOTE This standard addresses the validation of hydraulic actuators. Electrical actuators are not precluded on HIPPS; however, their detailed design guidelines are outside the scope of this RP. Electrical actuators are deemed in conformance with this standard only if they meet the performance design criteria and validation requirements established for hydraulic actuators.

A design that undergoes a substantive change is a change identified by the manufacturer or other, which affects the performance of the product in the intended service condition. This may include changes in fit, form, function, or material. A design that undergoes a substantive change becomes a new design requiring retesting. This shall be recorded, and the manufacturer shall justify whether or not requalification is required.

For an example SIL calculation, refer to Annex A.

9.2 Validation for HIPPS Closure Devices (Isolation Valve) and Actuator

9.2.1 Validation Testing

Validation testing of the HIPPS closure devices and actuators shall be performed on prototypes or production models of equipment made in accordance with API 17D for operating cycles, internal differential pressure cycles, temperature cycles, and hyperbaric (external) pressure cycles, level of Performance Requirement 2 (PR2).

The HIPPS closure devices and actuators should be validation tested in accordance with API 6A/17D under full design load (e.g. internal bore differential pressure), with no failures in performance or sealing criteria established under API 6A.

Validation testing should confirm the performance of the valves with respect to any HIPPS related performance standard.

9.2.2 Scaling

If the size of a HIPPS closure valve/actuator is not specifically performance verified, then the scaling rules which follow API 17D shall not be used to cite a qualified HIPPS closure valve/actuator to validate the new size. Each new size of valve/actuator shall be individually validation tested.

In some cases, the HIPPS closure valve/actuator may be used in a pipeline or flowline application. In these instances the valve’s bore may have to be resized (other than the nominal sizes listed in API 6A or API 17D) to be closer to the line pipe inner diameter to better accommodate pipeline pigging operations.

9.3 Validation for Monitor/Bleed, Bypass, Injection Valves

9.3.1 General

The following validation and scaling shall apply.

9.3.2 Validation Testing

Validation testing of associated HIPPS valves and actuators shall be performed on prototypes or production models of equipment made in accordance with API 17D for operating cycles, internal differential pressure cycles, temperature cycles, and hyperbaric (external) pressure cycles, Level PR 2. Validation testing shall confirm the performance of the valves with respect to any HIPPS related performance standard.

9.3.3 Scaling

If the size of an associated HIPPS valve is not specifically performance verified, then the scaling rules which follow API 17D shall not be used to cite a qualified valve to validate the new size. Each new size of valve/actuator shall be individually validation tested.

9.4 Validation for DCV

The DCV directs hydraulic control fluid to the actuator of the barrier valve. Validation testing of the DCV shall be performed on prototype or production model of equipment made in accordance with this standard to verify that the performance requirements specified for pressure, temperature, and mechanical cycles are met in the design of the product. Proper venting of the function line shall be provided for during these tests.

The following tests shall be performed on a single qualification valve; more than one valve may be subjected to these qualification tests.

— Cycle Testing—The cycle testing shall be performed with the DCV hydraulic supply at the maximum rated pressure and a control fluid cleanliness of SAE AS 4059, Class 6, B through F or better.

— The DCV shall be cycled 10,000 times—The pressure on the function line shall be monitored and shall drop to atmospheric pressure after each cycle to ensure full venting.

— Cycle Testing, Contaminated Fluid—The cycle testing shall be performed with the DCV hydraulic supply at the maximum rated pressure and a control fluid cleanliness of SAE AS 4059, Class 10. The valve shall be cycled 1000 times. The pressure on the function line shall be monitored and shall drop to atmospheric pressure after each cycle to ensure full venting.

— Hyperbaric Testing at Low Temperature—The valve shall be tested in a hyperbaric chamber at a test pressure that simulates the water depth rating of the DCV. The hydraulic supply pressure for these tests shall be at the maximum rated pressure of the DCV. The control fluid should be clean to SAE AS 4059 Class 6, B through F. The water in the test chamber should be cooled to 2 °C (35 °F) or below. The DCV shall be cycled 100 times. The pressure on the function line shall be monitored and shall drop to atmospheric pressure (hyperbaric test pressure) after each cycle to ensure full venting.

9.5 Validation of Sensors, Logic Solvers, and Control System Devices

Control system components or devices (including but not limited to: pressure sensors, flow measurement sensors, chemical injection or monitoring ports, hydraulic mounting plates, stab plates, electrical or fiber optic connectors, programmable devices etc.) are considered to be Type A or Type B systems as defined by IEC 61508, Part 2.

Relevant failure data for these components should be used when the PFD is required. The failure data shall be properly documented, and the assumptions for the data shall be given. Both the failure rate for dangerous undetectable failures (λ_{du}) and the total failure rate (λ_{TOT}) or SFF are required.

NOTE λ_{TOT} only includes critical failures (i.e. failures that affect the safety function). If relevant, parameters used for assessing common mode/common cause failures (e.g. β-factors) are included and documented as part of the failure data.

Failure data may be obtained in three different ways, or in a combination, of the following.

a) Experience data from same or similar applications.

— The data shall be based on components that are used under similar environmental and operating conditions, and the design of the components shall be identical.

— For this type of failure data source the number of performed tests of the relevant safety function shall be given together with how many of these functional tests that resulted in failure. Further, the time interval between these functional tests shall be given. If the data are collected from several sources, it is preferred that this information is given per data source.

— The PFD and λ_{du} estimates should be conservative (IEC 61508 requires that any failure rate data used shall have a statistical confidence level of at least 70 %).

— It is not sufficient to know the operating time of the components, the basis for the failure data estimation should be as given above.

a) Third-party certificate or similar.

NOTE Failure rates in certificates tend to be “predicted” values rather than collected field data. As such, they may bear no relation to how the item performs in real situations. It is therefore important not to place too much reliance on such information, particularly for field items such as sensors and valves. Predictions for these items tend to be ‘optimistic’ and field data are to be preferred.

— All requirements and assumptions relevant for the certificate shall be documented. Thus, in addition to the certificate itself, the documentation shall include the background information (assessment report or similar).

a) Assessment of the component/system based on failure data from generic sources.

— The assessment shall be properly documented through a fault tree analysis including common cause effect. The assessed component/system shall have the same type of use, the same safe state, and the same design with respect to safe state [i.e. normally energized (NE) versus normally de-energized (NDE)]. Further, if the assessment is based on published reliability handbook predictions or similar, all necessary parameters (e.g. environment and quality) shall be relevant for the current application, and shall be stated as part of the documentation.

— A safety manual document should be prepared by the manufacturer of the logic solver [also referred to as a trigger module or programmable electronic system (PES)], which fully documents the compliance with IEC 61508 by an independent testing agency. The safety manual should also state the maximum SIL the logic solver may be incorporated into, the intended HIPPS SIS, and describe the configurations and environment in which the logic solver may be incorporated and operated within the HIPPS SIS.

— Some subsea control architectures feature parallel redundant circuits or systems which are intended to augment hardware reliability, lower the likelihood of spurious trips or errors, or increase the interval between subsea intervention and maintenance events. Safety manuals illustrating a single logic solver application may be used as the documentation to validate the logic solvers used in these dual-parallel control system architecture applications provided the control system supplier/integrator can demonstrate the parallel or redundant

configuration does not introduce additional dangerous undetectable failure modes, nor safety manual stated PFD, HFT, SFF values have been compromised. Validation should be per validation testing performed by bench testing two or more logic solvers in the intended parallel circuit configuration and under the same operating conditions stated in the safety manual document.

9.6 Validation of HIPPS Final Element

Performance of HIPPS final element components (valves) are often drawn from API 6A and API 17D cycle test validation test requirements, since these components are of limited quantity and statistical averages may not be readily obtained. Therefore, this calculation method may be used to estimate mean time between failure (MTBF) and SIL until sufficient field data become available, as outlined in API 17N.

The estimation method assumes that API Spec. 6A and API Specification 17D performance test failures are random occurrence with zero failures during testing, as established by these industry standards. Therefore to estimate reliability, a chi-square (χ^2) distribution is used to estimate the uncertainty of the reliability estimate (chi-square distribution assumes failures occur at random as opposed to infantile or wear out failures).

The HIPPS final element assembly should be validation tested under full design load (e.g. internal bore differential pressure), with no failures in performance or sealing criteria established under API 6A. The validation testing should also include demonstration of closing and opening times to meet specified requirements. This performance test should be in addition (not cumulative) to any component validation test discussed above.

The HIPPS final element should include the HIPPS closure device (isolation valve assembly), hydraulic control valve, and quick exhaust valves used on HIPPS closure device and its actuator plumbing. The plumbing shall be equivalent or more conservative than the plumbing used in actual system with the consideration of pipe line size, length, elbows, tees, number of bends. The HIPPS final element used for validation testing may be a prototype or production model.

10 Installation and Commissioning

10.1 General

Installation is defined as that period after manufacture and testing where the HIPPS is moved to its service location, fixed in place, mechanically completed (i.e. completed as per all design documents and approved changes), and hooked up to the system to be protected.

Commissioning includes activities from testing through introduction and filling with produced fluids.

The HIPPS should be designed to allow installation and commissioning activities to take place without compromising the SIL. The HIPPS shall be installed and commissioned to maintain the SIL required by the design. MOC shall be maintained throughout the installation and commissioning process to ensure that any changes found necessary during these phases of the work do not compromise the specified SIL and are reflected in updates to the SRS per 4.6.

To facilitate the installation and commissioning of the HIPPS, the transportation and installation load conditions and any underlying assumptions and interface definitions for which the design was produced shall be transmitted to the installation and commissioning entities.

10.2 Planning

10.2.1 General

Planning should be performed to define all activities required for installation, mechanical completion, hookup, and commissioning/verification prior to undertaking the work.

Written procedures for the work should be independently reviewed for the installation of the HIPPS. The procedures should be supported by calculations, where necessary, to show that the HIPPS can be installed safely and without damage. The installer should carry out a risk assessment study to identify potential deviations from the plan and develop contingency procedures for common deviations. Procedures shall cover the required level of authorization needed for any changes.

Planning shall encompass MOC procedures for handling nonconformities where the installation and commissioning does not conform to the design assumptions and requirements.

10.2.2 Testing and Commissioning Planning

The following items shall be included in the plans as a minimum:

- all testing and commissioning activities, including verification of the HIPPS with respect to the safety requirements specification and implementation and resolution of resulting recommendations;
- testing of all relevant modes of operation of the process and its associated equipment, including:
  - preparation for use including setting and adjustment;
  - start-up, teach, automatic, manual, semiautomatic, and steady state of operation;
  - resetting, shutdown, and maintenance;
  - reasonably foreseeable abnormal conditions;
  - the procedures, measures, and techniques to be used;
  - reference to criteria to be met (e.g. cause and effect chart, system control diagrams);
  - when the activities shall take place; and
  - the persons, departments, and organizations responsible for the activities and levels of independence required.

Additional planning for verification of the safety application software should identify safety-related software which needs to be validated for each mode of process operation including:

- information on the strategy for the verification, including:
  - manual and automated techniques;
  - static and dynamic techniques; and
  - analytical and statistical techniques;
- in accordance with strategy, the techniques and procedures to be used for confirming that each SIF conforms with:
  - specified requirements for the software SIFs;
  - specified requirements for software safety integrity; and

  - required environment in which the activities are to take place (e.g. for tests this would include calibrated tools and equipment);

- pass/fail criteria for accomplishing software verification, including:

  - required process and operator input signals with their sequences and their values;

  - anticipated output signals with their sequences and their values;

  - other acceptance criteria (e.g. memory usage, timing and value tolerances); and

  - the policies and procedures for evaluating the results of the verification and for remedial measures in the event of failures.

10.3 Installation

10.3.1 General

Installation should be performed according to the previously prepared plans and procedures.

10.3.2 Pre-installation Survey

Before the installation, a survey shall be carried out to confirm that the seabed in the vicinity of the installation is free of any obstructions or other factors that could adversely affect or be affected by the installation or operation of the HIPPS. The survey shall also confirm the position of any adjacent facilities or installation aids, especially ones with which the HIPPS interfaces.

The survey shall be carried out using positioning and navigation equipment equivalent to that which is to be used during the installation operations.

The installer shall propose suitable methods of seabed preparation to rectify any conditions contrary to those for which the HIPPS is designed and shall carry out that preparation.

10.3.3 As-built Survey

An as-built survey should be performed to document the installed condition of the equipment. The survey should be documented in a report containing text and illustrations as required. The survey shall cover the following:

- general conditions;

- absolute location;

- relative location with respect to other local facilities and equipment;

- variations from design;

- repairs; and

- inspection and test results.

10.4 Commissioning

10.4.1 General

Implementation/commissioning activities shall be performed in accordance with the safety requirements, detailed design, and planning documents. Any deviations from these documents shall be evaluated for impact on the SIL and on any assumptions made with regard to performance to ensure no degradation of function.

10.4.2 Testing and System Verification

Testing and commissioning shall demonstrate that the HIPPS meets requirements of the SRS and works as planned in the installed system.

Subsequent to installation, tests should be conducted to verify that the entire system, including the final shutdown of valves and controls, is designed and installed to provide proper response to the abnormal conditions for which it was designed. Such verification should confirm, for example, that:

— response time is as rapid as required by design;

— system functions (e.g. closure) take place; and

— other performance factors are within specified design limits.

Before initial operation of the HIPPS, after a shut-in of over 30 days, after a modification, or after recommissioning, the system should be checked to verify that each component is installed, operable, performs its design function, and if applicable, is calibrated for the specific operating conditions.

A safety analysis function evaluation (SAFE) chart should be developed to provide a checklist for the initial design and installation verification. Each sensing device should be listed and its respective control function indicated. It shall be determined that a safety device is operable, properly calibrated, and accomplishes the design control function within the prescribed time period. This fact should be noted on the SAFE chart. When all initiating devices have been tested and their functional performance confirmed, the design and installation is verified/validated.

HIPPS testing should be performed in accordance with the functional requirements of API 14C, while recognizing differences due to the submarine environment.

Pressure integrity of HIPPS and associated upstream and downstream pipelines and equipment should be confirmed by pressure testing. Testing should be done to a minimum of 1.25 times their respective MAWPs or governing codes and regulations for the respective sections. Tie-ins should undergo alternative inspections and leak testing where they cannot be tested as part of the overall system.

10.4.3 Testing and Commissioning Activities

HIPPS safety verification is here defined as all activities necessary to validate that the installed and mechanical completed HIPPS and its associated instrumented functions, meets the requirements as stated in the SRS.

Measuring instruments used for testing shall be calibrated against a specification traceable to a national standard or to the manufacturer’s specification.

Activities should confirm that:

— the SIS performs under normal and abnormal operating modes (e.g. start-up, shutdown, etc.) as identified in the SRS;

— adverse interaction with the basic process control system and other connected systems do not affect the proper operation of the SIS;

— the SIS properly communicates (where required) with the basic process control system or any other system or network;

— sensors, logic solver, and final elements perform in accordance with the SRS, including all redundant channels;

— documentation reflects the installed system;

— the SIF performs as specified on bad (e.g. out of range) process variables;

— the proper shutdown sequence is activated;

— the system provides the proper annunciation and proper operation display;

— computations that are included in the SIS are correct;

— the reset functions perform as defined in the SRS;

— bypass functions operate correctly;

— manual shutdown systems operate correctly;

— the proof test intervals are documented in the maintenance procedures;

— diagnostic alarm functions perform as required; and

— the system performs as required on loss of power or a failure of a power supply and when power is restored, the system returns to the desired state.

Prior to using the HIPPS for its intended purpose and after the testing activities are complete, the following activities shall be carried out:

— all process isolation valves shall be set according to the process start-up requirements and procedures;

— all test materials (e.g. fluids) shall be removed; and

— a final shutdown test shall be performed.

10.4.4 Testing and Commissioning Documentation

Documentation shall include the following as a minimum:

— the HIPPS verification plan being used;

— the SIF under test (or analysis), along with the specific reference to the requirements identified during HIPPS verification planning;

— tools and equipment used, along with calibration data;

— the results of each test;

— the test specification used;

— the criteria for acceptance of the tests;

— the version of the HIPPS being tested;

— any discrepancy between expected and actual results;

— the analyses performed and the decisions taken on whether to continue the test or issue a change request, in the case when discrepancies occur; and

— in case of discrepancies between expected and actual results, the analyses performed and the decisions taken should be available as part of the results of the hardware and software verification, including recording whether it was decided to continue the verification or issue a change request, and return to an earlier part of the development lifecycle.

10.4.5 Repairs

Any damage detected during inspections should be repaired using approved procedures, and retests performed as necessary. Any modifications made during repairs shall go through the MOC process, have full documentation, and undergo approval/verification by the manufacturer, when necessary.

10.4.6 Introduction of Product

The system should be started without causing a greater level of risk than normal operation. Due regard for differences from normal operation should be considered during HIPPS design and when developing and executing commissioning procedures.

Differences that might occur are as follows:

— use of the system to produce well cleanup fluids;

— variations in temperature and pressure during start-up;

— temporary injection of chemicals; and

— initial conditions and sequence of operation of equipment.

Commissioning procedures and activities should consider the operation of upstream equipment and downstream pipelines to ensure that proper protection of the downstream system is maintained at all times.

Annex A
(informative)

Estimating SIL for Overall HIPPS Safety Instrumented Function

A.1 General

The demonstration that a safety instrumented function achieves a specified safety integrity level requires the following aspects be addressed: (a) the target failure measure (e.g. Probability of Failure on Demand), (b) Architectural Constraints: Hardware Fault Tolerance (HFT), and Systematic Safety Integrity. The reader is strongly recommended to consult the relevant international standards (IEC 61508 and IEC 61511) for more detail on these matters.

The section below is not intended to be exhaustive and is provided as introductory guidance. Calculations shall always be carried out by persons competent to understand the limitations of particular equations and be able to include any additional factors that may be necessary for a specific situation.

Failure rate data should come from a validated source. Care should be taken in selecting the failure rate data that are relevant to the safety function.

For information on human contributions to and interactions with a safety instrumented function, refer to Annex B.

A.2 Probability of Failure on Demand

A.2.1 General

A safety integrity level (SIL) applies to a complete safety instrumented function (SIF). Individual elements or subsystems that form part of a safety instrumented function may have a SIL capability that makes them suitable for use at certain integrity levels but that suitability does not confer the integrity level from either the element or subsystem on the overall function.

NOTE 1 See IEC 61508-4 definition of safety integrity level (SIL).

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element, or component. The correct interpretation of the phrase “SIL n safety-related system” (where *n* is 1, 2, 3, or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to *n*.

This section provides an example safety instrumented function that is based on Figure 1 for a Typical Subsea Production HIPPS. This example safety instrumented function is shown in block diagram form in Figure A.1.

Calculation of the average probability of failure on demand (PFD_{avg}) is carried out using Simplified Equations.

NOTE See ISA-TR84.00.02-2002—Part 2 for some examples of simplified equations.

However, it is important to appreciate that simplified equations exclude a number of complex factors, some of which may need to be included in order to represent properly the safety instrumented function in calculation. These include features such as: imperfect testing, partial testing, diagnostics, Mean Time to Repair (MTTR), imperfect repair, down-time for testing, designing for availability as well as safety, automatic degradation of voting, etc.

For an example of a PFD_{avg} calculation, refer to Annex C.

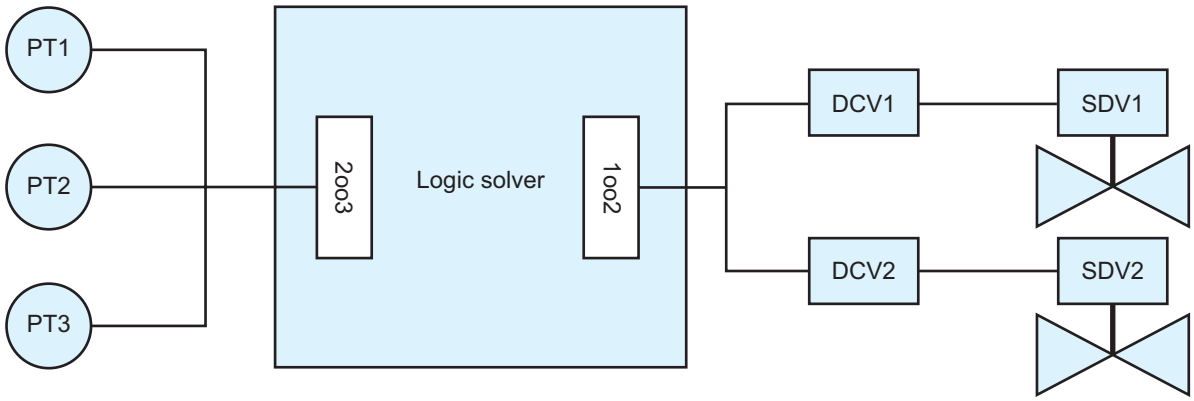

Figure A.1—Safety Instrumented Function (SIF) Example

A.2.2 Input Section

The input section has three channels, with each channel comprising an individual pressure sensor. For a single channel the equation for independent failure probability is:

$$PFD_{avg} = 0.5 \times \lambda_{DU(i)} \times T_{(i)} \quad (1)$$

In this equation, $\lambda_{DU(i)}$ is the dangerous undetected failure rate for one input channel and $T_{(i)}$ is the proof test interval used for all input channels.

NOTE If $\lambda_{DU(i)}$ is in units of “per year” then $T_{(i)}$ must be expressed in units of “years”.

The three channels are voted on a 2oo3 basis for success. The equation for independent failure probability is:

$$PFD_{avg} = 4\,[(PFD_{avg} \text{ for a single channel})^2] \quad (2)$$

NOTE The factor “4” above is specific to 2oo3 voting and changes depending on the voting architecture being addressed.

To this must be added the PFD_{avg} for common cause or dependent failure. The equation for dependent failure probability is:

$$PFD_{avg} = \beta\,(PFD_{avg} \text{ for a single channel}) \quad (3)$$

β in the above equation is the beta factor used for dependent failure calculation [6]. The overall PFD_{avg} for the input section is therefore:

$$PFD_{avg} \text{ (Input Section)} = 4\,[(0.5 \times \lambda_{DU(i)} \times T_{(i)})^2] + \beta\,(0.5 \times \lambda_{DU(i)} \times T_{(i)}) \quad (4)$$

A.2.3 Logic Section

The logic section can be treated as a single unit, and with calculation of PFD_{avg} using an equation similar to that above:

$$PFD_{avg} \text{ (Logic)} = 0.5 \times \lambda_{DU(L)} \times T_{(L)} \quad (5)$$

6 Assessment of an appropriate beta factor for a specific situation is a specialized task. It depends on the voting architecture, whether the channels are identical or have important differences, and a number of other factors.

In this equation, $\lambda_{DU(L)}$ is the dangerous undetected failure rate for the logic solver and $T_{(L)}$ is the proof test interval used.

A.2.4 Output Section

The output section has two channels, with each channel comprising a solenoid valve and a process trip valve. The PFD_{avg} for a single channel is again determined using the equation:

$$PFD_{avg} = 0.5 \times \lambda_{DU(o)} \times T_{(o)} \quad (6)$$

In this equation, $\lambda_{DU(o)}$ is the dangerous undetected failure rate for one input channel and $T_{(o)}$ is the proof test interval used for all output channels.

The two channels are voted on a 1oo2 basis for success. The equation for independent failure probability is:

$$PFD_{avg} = 4/3\ [(PFD_{avg} \text{ for a single channel})^2] \quad (7)$$

To this must be added the PFD_{avg} for common cause or dependent failure. The equation for dependent failure probability is:

$$PFD_{avg} = \beta\,(PFD_{avg} \text{ for a single channel}) \quad (8)$$

β in the above equation is the beta factor used for dependent failure calculation. The PFD_{avg} for the output section is therefore:

$$PFD_{avg}\ (\text{Output Section}) = 4/3\ [(0.5 \times \lambda_{DU(o)} \times T_{(o)})^2] + \beta\,(0.5 \times \lambda_{DU(o)} \times T_{(o)}) \quad (9)$$

A.2.5 Overall Calculation

The overall PFD_{avg} for the safety instrumented function is then the sum of the values for the three sections:

$$PFD_{avg}\ (\text{Overall}) = PFD_{avg}\ (\text{Input Section}) + PFD_{avg}\ (\text{Logic}) + PFD_{avg}\ (\text{Output Section})$$

It is this overall PFD_{avg} that is used when assessing whether the required safety integrity level has been achieved.

NOTE There are other aspects that need to be considered before concluding that the required integrity has been achieved. For a specified safety integrity level to be claimed, there are also requirements for Hardware Fault Tolerance (HFT) and Systematic Integrity that need to be met.

A.2 Diagnostics

When considering an item of equipment, it is often considered that a proportion of the dangerous failures (λ_D) will be detected by some form of diagnostics. The proportion of dangerous failures claimed to be detected during normal operation is then referred to as the Diagnostic Coverage (DC). It follows that the undetected dangerous failure rate (λ_{DU}) can be expressed as:

$$\lambda_{DU} = \lambda_D - \lambda_{DD}$$

$$\lambda_{DU} = \lambda_D\,(1 - DC)$$

Where λ_{DD} is the failure rate associated with detected dangerous failures.

Thus with a figure of 95 % for diagnostic coverage, the value of λ_{DU} is only 5 % of the dangerous failure rate (λ_D). The use of diagnostic coverage allows for smaller values of λ_{DU} to be used for PFD_{avg} calculations compared with having no diagnostic coverage when $\lambda_{DU} = \lambda_D$.

However, whilst a claim for diagnostic coverage can be made, it should be noted that the diagnostic feature has a dangerous failure rate (i.e. it can stop working without the stoppage being evident) and it is often difficult to arrange a form of proof test to demonstrate (a) that the diagnostics are fully working, and (b) that they are still monitoring all the failure modes for which they are claimed.

Furthermore, in calculations involving diagnostic coverage the dangerous failure rate of the diagnostics is often overlooked.

The inclusion of diagnostic coverage is therefore something that should receive careful thought before it is claimed as a means of reducing the undetected dangerous failure rate.

Annex B
(informative)

Human Contribution During Operation

A safety instrumented function (SIF) requires human interaction throughout its operational lifetime. This can be in the form of testing and calibration and also in terms of any maintenance and repair that is necessary. Humans are fallible and cannot be guaranteed to carry out tasks 100 % successfully every time. There is, therefore, the potential for an SIF to be left in a non-functioning state following human interaction with it.

For example, if there is a bypass line with a ROV operated block valve around a trip final element valve then the question arises: “when the bypass valve was last used, what is the probability that it was left in the open state and hence leaving the safety function a non-functioning state?”

Assessment of the probability of omission for a simple step in a procedure may well be of the order of 0.005, depending on the conditions under which the task is carried out and various other factors. It can be seen that this probability when compared with that for a SIL 1 function (0.01 to < 0.1) is not going to make a significant impact on the overall performance of the function. However, for a SIL 2 function (0.001 to < 0.01) it is of the same order of magnitude; it could even move the overall performance of a SIL 2 function into the range for SIL 1. For a potential SIL 3 function, it would prevent achieving a failure probability in the SIL 3 range (0.0001 to < 0.001).

Therefore, it is highly important to consider the impact of human error on the performance of an SIF. You cannot simply say to a person who is about to calibrate a function intended to achieve SIL 3, “please can you be 100 times more careful when working on this SIL 3 function than you are when working on the SIL 1 functions?” There needs to be careful consideration of the nature of the tasks associated with SIFs and the conditions under which those tasks are to be carried out, with the aim of tailoring the tasks so that their contribution to the probability of failure of the function is sufficiently small and the required integrity can be achieved.

Annex C
(informative)

Example PFD_{avg} Calculation

This is an illustration of a calculation to show how the PFD_{avg} is reached for the whole safety instrumented function (SIF) and hence the safety integrity level (SIL). See Table C.1.

Table C.1—Data for the Calculations[a]

Item	Description	Value [b]
Sensor (PT)	Undetected Dangerous Failure Rate (λ_{DU})	0.02 per year
Logic Unit	Probability of Failure on Demand	0.0001
Solenoid Valve (SOV)	Undetected Dangerous Failure Rate (λ_{DU})	0.02 per year
Trip Valve (XZV)	Undetected Dangerous Failure Rate (λ_{DU})	0.03 per year
Beta Factor	Common Cause Proportion	10% [c]
Test Interval	Proof Test Interval (T)	1 year

[a] These data would be typical of actual field data from the process sector of industry for "non-smart" equipment other than the logic unit.

[b] The data here are provided only to illustrate the method of calculation. It is vital that calculations for a specific safety instrumented function reflect the failure rate expected for the equipment items in the particular application. The data used are derived from relevant field performance not theoretical predictions. Appropriate traceability is provided to support data used in calculations.

[c] Ten percent represents a conservative value for identical items in close proximity.

PFD_{avg} (Input Section) $= 4\,[(0.5 \times \lambda_{DU(i)} \times T_{(i)})^2] + \beta\,(0.5 \times \lambda_{DU(i)} \times T_{(i)})$

$= 4\,[(0.5 \times 0.02 \times 1)^2] + 0.1\,(0.5 \times 0.02 \times 1)$

$= 0.0004 + 0.001$

$= 0.0014$

PFD_{avg} (Logic) $= 0.0001$

PFD_{avg} (Output Section) $= 4/3\,[(0.5 \times \lambda_{DU(o)} \times T_{(o)})^2] + \beta\,(0.5 \times \lambda_{DU(o)} \times T_{(o)})$

$= 4/3\,[(0.5 \times (0.02 + 0.03) \times 1)^2] + 0.1\,(0.5 \times (0.02 + 0.03) \times 1)$

$= 4/3\,[(0.5 \times 0.05 \times 1)^2] + 0.1\,(0.5 \times 0.05 \times 1)$

$= 0.00083 + 0.0025$

$= 0.00333$

PFD_{avg} (Overall) $= 0.0014 + 0.0001 + 0.00333$

$= 0.00483$

Thus from hardware failure rates and an annual test interval, this function achieves an average probability of failure on demand in the range corresponding to that required for SIL 2.

The test interval used in the calculations can be a proposed value or the actual value being used for proof testing. In any situation, T should be significantly less than $1/D$, where D is the demand rate on the safety instrumented function. T should also be significantly less than $1/\lambda_{DU}$.

Bibliography

[1] API Recommended Practice, 14C, *Analysis, Design, Installation and Testing of Basic Surface Safety Systems on Offshore Production Structures*

[2] API Specification 7-1, *Specification for Rotary Drill Stem Elements*

[3] API Specification 5CT, *Specification for Casing and Tubing*

[4] API Specification 16A, *Specification for Drill-through Equipment*

[5] API Specification 16R, *Marine Drilling Riser Couplings*

[6] ANSI/ASME B16.11[7] [8], *Forged Fittings, Socket-Welding and Threaded*

[7] DOT Title 49, *Code of Federal Regulations* (*CFR*) Part 192 [9], *Transportation of Natural and Other Gas by Pipeline: Minimum Federal Safety Standards*

[8] API Specification 6H, *Specification on End Closures and Swivels*

[9] OLF 70 [10], *Recommended guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities of the Norwegian Continental Shelf*

[10] DNV-RP-B401 [11], *Offshore Standard, Cathodic Protection Design*

[11] NACE RP 0176 [12], *Corrosion control of submerged areas of permanently installed steel offshore structures associated with petroleum production*

[12] ASNT SNT-TC-1A [13], *Personnel Qualification and Certification in Nondestructive Testing*

[13] API Standard 520, *Sizing, Selection, and Installation of Pressure Relieving Devices in Refineries, Part I—Sizing and Selection*

[14] ANSI/ASME B31.4, *Pipeline Transportation Systems for Liquid Hydrocarbons and Other Liquids*

[15] DNV-OS F101, *Submarine Pipeline Systems*

[16] API Recommended Practice 17N, *Recommended Practice for Subsea Production System Reliability and Technical Risk Management*

---

7 American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, New York 10036, www.ansi.org.
8 ASME International, 2 Park Avenue, New York, New York 10016-5990, www.asme.org.
9 U.S. Department of Transportation,1200 New Jersey Ave, SE, Washington, DC 20590, www.dot.gov.
10 Norwegian Oil Industry Association, P.O. Box 8065, 4068 Stavanger, Norway, www.olf.no.
11 Det Norske Veritas, Veritasveien 1, 1322, Hovik, Oslo, Norway, www.dnv.com.
12 NACE International (formerly the National Association of Corrosion Engineers), 1440 South Creek Drive, Houston, Texas 77084-4906, www.nace.org.
13 American Society for Nondestructive Testing, 1711 Arlingate Lane, P.O. Box 28518, Columbus, Ohio 43228, www.asnt.org.

AMERICAN PETROLEUM INSTITUTE

1220 L Street, NW
Washington, DC 20005-4070
USA

202-682-8000

Additional copies are available online at www.api.org/pubs

Phone Orders:	1-800-854-7179	(Toll-free in the U.S. and Canada)
	303-397-7956	(Local and International)
Fax Orders:	303-397-2740	

Information about API publications, programs and services is available on the web at www.api.org.

Product No. G17O02