API 521 8th Edition Ballot Item 6

REBALLOT

Annex E Updates
(Work Item 17)

Instructions to Voters/Commenters

- Please limit your comments to the red- and blue- lined portions of the ballot only.
  - Red indicates modifications to the previously balloted wording.
  - Blue indicates new text.
- If you are voting negative with multiple comments, please indicate which comment(s) is the reason for your negative vote, otherwise API's balloting system will categorize all of your comments as negative.

Thanks to Hasinah Hanafi and the work group for their efforts.

Melissa Marashi (Chevron)
David Fenton (ExxonMobil)

API 521 Task Force Chairs

Definitions

high-integrity protection system

HIPS

Safety instrumented system (SIS) that is designed, built, and maintained to a sufficiently high safety integrity level (SIL) to protect equipment against exceeding the design parameters.

high-integrity pressure protection system

HIPPS

A high integrity protection system (HIPS) designed to prevent overpressure of equipment and/or piping in lieu of or in combination with a pressure-relief device.

3.1.69

safety instrumented system

SIS

~~**high-integrity protection system**~~

~~**HIPS**~~

System composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are met.

NOTE Other terms commonly used for an SIS include emergency shutdown system (ESD, ESS), safety shutdown system (SSD), and safety interlock system (see E.3.3.1).

4.4.7 Overfilling

4.4.7.1 General

Many process or surge vessels, including columns and towers, have a liquid level present during normal, start-up, or shutdown conditions. Experience has shown that this equipment can be overfilled under certain conditions. If the source pressure of a liquid feed or supply line can exceed the relief device set pressure and/or the design pressure of the equipment, then overfilling shall be evaluated. System design options to deal with liquid overfill include but are not limited to:

a) increasing the system design pressure and/or PRD set pressure within pressure design code allowances;
b) designing a pressure-relief system that can safely accommodate the overfill (including the effects of operator intervention response as discussed in 4.2.5);
c) installing a safety instrumented system (SIS) or high-integrity protective system (HIPS) to prevent the liquid overfill (see Annex E for additional information ~~on SISs~~).

4.4.7.2 Mitigation Measures

When designing the system to mitigate liquid overfill, the following can affect the design and shall be evaluated:

a) risk of failure of the operator to respond properly;
b) operator training and operating procedures that include the expected response of instrumentation;
a) EXAMPLE A differential pressure or displacer-level measurement will read low compared to actual level if the
b) fluid-specific gravity is less than the design-specific gravity. This can mean that the indicated level cannot reach 100 % even
c) if the actual level is well above the measured range.
d) availability of instrumentation that is required for adequate operator intervention;
e) availability of instrumentation that is required for SIS or HIPS response;

Annex E
(informative)

High-integrity Protection Systems (HIPS)[1]

E.1 Introduction

Traditional methods of pressure relief employ a mechanical device such as a PRD to prevent the pressure in ~~any piece of~~ equipment from exceeding the maximum allowable accumulated pressure. As discussed in section 4.2.6, where overpressure protection via ~~mechanical device~~ PRD is impractical, a different approach to overpressure protection is the use of an instrumented system. HIPS involve an arrangement of instruments, final control elements (e.g. valves, switches, etc.), and logic solvers configured in a manner designed to mitigate overpressure incidents by removing the source of overpressure or by reducing the probability of an overpressure contingency to such a low level that it is no longer considered to be a credible case. The rationale of using HIPS should be documented and approved by the owner/operators ~~which inline~~ to ensure it aligns with requirements specified in codes ~~for~~ of construction.

~~With appropriate levels of redundancy, a HIPS can be designed to achieve a level of availability equal to or greater than a mechanical relief device. However,~~ The application of HIPS requires a number of special procedures within the design process to ensure an adequately safe HIPS design and it requires particular attention during its operational life such as maintenance, testing and inspection. For these reasons, the decision to implement a HIPS on a given project should be made with a great deal of caution and careful consideration. Note that ~~it can be~~ a higher level of integrity may be necessary for the HIPS ~~required overpressure protection availability to be higher~~ than that provided by a single mechanical relief device.

This annex provides a discussion of the elements of a HIPS, the applicable codes and standards associated with HIPS and the procedures which should be followed when implementing HIPS.

E.2 Background

E.2.1 Elements of a HIPS

A HIPS includes field instruments (e.g. sensors), logic solving devices (e.g. safety system logic solver, relays, etc.), final control elements, power supply and inspection, testing, and maintenance procedures. The boundaries of a HIPS incorporate all aspects from the sensor to the final element. In addition to automatic activation of ~~HIPPS~~ HIPS, ~~providing~~ a supplemental manual activation of ~~HIPPS~~ HIPS ~~can be considered~~ may also be provided~~, either through manual activation of ESD system or any other means~~.

E.2.2 Application of HIPS

E.2.2.1 Principal Uses

There are six principal uses of a HIPS:

---

[1] This document does not differentiate between High Integrity Protection System (HIPS) and High Integrity Pressure Protection System (HIPPS).

a) to eliminate a particular overpressure scenario from the design basis of the relief device.

b) to reduce the required flowrate for a credible scenario to a rate within the capacity of ~~an~~ one or more existing relief devices.

c) to eliminate the need for a ~~particular~~ relief device.

d) to provide system overpressure protection where a relief device is ineffective ~~or undesired~~.

e) to reduce the probability that several relief devices will have to operate simultaneously, thereby allowing for a reduction in the size of the disposal system (e.g., reduce the flare backpressure or radiation).

~~f) to reduce the demand rate frequency on a relief device consequently reducing the risk.~~

There is a large amount of overlap between these principles of HIPS applications; a particular application of HIPS can pertain to more than one of the above categories.

In some situations, the provision of a HIPS ~~to avoid more extensive relief system or flare modifications or design may be a more cost-effective option.~~ can be a more cost-effective option by avoiding more extensive relief system or flare modifications or design. Both initial and life cycle costs associated with testing and maintenance should be considered. ~~The provision of a HIPS involves both initial and life-cycle costs associated with testing and maintenance.~~ Moreover, HIPS can be designed to achieve a higher level of ~~availability and~~ reliability than a mechanical relief device by using components designed to have very low failure-to-danger rates and that are designed to primarily fail safe by incorporating appropriate levels of redundant instrumentation and by ensuring that the HIPS is inspected and tested on a regular basis. Thus, a HIPS can be used as a risk-reduction measure for particularly high-risk process units (e.g. those that involve acutely toxic materials). ~~In some cases, a HIPS can be used in concert with a relief device (where the relief device is generally a "backup" to the HIPS) to achieve especially high levels of protection.~~

Note, however, that the ~~lifecyle~~ lifecycle management and ongoing cost of ownership of a HIPS should be taken into account. This includes costs of routine testing of the HIPS versus routine PRD maintenance. This ongoing cost rises ~~disproportionately~~ with the SIL level (see 3.1.71, 3.1.72, and E.3.3.2).

E.2.2.2 Important Considerations

Some important considerations in HIPS design and implementation ~~are as follows~~ include, but are not limited to:

a) The HIPS may reduce the sources of overpressure, but not completely eliminate them. For example, successful operation of a HIPS system to shut off fuel to a fired heater does not eliminate all heat flux to the heater tubes since there is residual heat contained in the furnace-wall refractory.

b) ~~When there are few numbers of HIPS being installed in one common facility to reduce the total design capacity of flare system, consideration to perform transient analysis to determine the maximum transient relief load will ensure correct relief rate been selected in designing the flare system or method as proposed in section 5.3.4.3 can be used if HIPS being used as flare reduction credit.~~ When HIPS are installed to reduce the total required capacity of the flare or disposal system, other loads, such as those resulting from basic process control system activation, residual energy sources, or other relief sources, may still be present and should be analyzed. See Section 5.3.4.3 for details around refinement of disposal system design load.

c) ~~Activating HIPS can result in a major shutdown or operational upset causing and thus incur the hazards associated with the shutdown and subsequently requirement to restart the facilities.~~ Activation of HIPS can lead to an operational upset, possible shutdown and unit restart, and all of the associated hazards.

d) The likelihood and consequence of the failure of a HIPS to properly function should be ~~considered~~ evaluated and compared to the owner's risk management criteria when deciding whether a HIPS is an acceptable ~~mitigation~~ prevention approach for the application under consideration. See Section E.4.2.

e) The likelihood and consequence of HIPS activation when not needed (spurious trip) should be evaluated. A spurious trip may result in unplanned unit shutdowns (and subsequent startups) creating additional opportunities for other overpressure scenarios and additional environmental discharges associated with both.

f) HIPS components should be independent of initiating causes and other safeguards.

g) HIPS should be designed with consideration for the instrumented system response time required to prevent overpressure.

h) Selection of instrumented system trip points should consider response time while minimizing the potential for spurious trips due to normal process variations. A safety factor may be applied to the determined minimum response time that considers the degree of uncertainty in predicting that time. Operational experience, modeling, or other means can be used to determine an appropriate instrument response time.

E.3 Relevant Regulations and Industry Standards

E.3.1 General

The user should obtain the latest edition of the documents referenced in this annex and review local jurisdictional applicability.

Relevant ~~international standards~~ references include but are not limited to ~~the following:~~ those listed in Table E.1.

Table E.1 — Industry Codes, Standards, and Practices

Applications	**~~Relevant Industrial Std~~ Industry Codes, Standards, and Practices**
Pressure vessels	- ASME Section XIII, Part 13 - ~~PED~~Pressure Equipment Directive 2014/68/EU Chapter 1, ~~and~~ Article 2 (HIPS referred to as SRMCR) - EN 764-7
Safety Instrumented ation system	- IEC 61508 - IEC 61511-1 (ANSI/ ISA 61511-1) - IOGP 443

Offshore facilities	- API 14 C (Annex E) - API 17O - API 17V

E.4 Procedures for Applying HIPS

E.4.1 General

The use of HIPS for any particular application has both advantages and disadvantages. Thus, for a given case, it is necessary to weigh the risk versus the benefit and make a well-considered, informed decision as to whether HIPS is the best option.

Table ~~E.1~~ E.2 — SIL and Average Probability of Failure ~~of~~ on Demand

Safety Integrity Level (SIL)		SIS Performance Requirements
ISA 61511-1	**IEC 61508**	**Average Probability of Failure on Demand** PFD_{avg}
1	1	~~10^{-1} to 10^{-2}~~ ≥ 10^{-2} to < 10^{-1}
2	2	~~10^{-2} to 10^{-3}~~ ≥ 10^{-3} to < 10^{-2}
3	3	~~10^{-3} to 10^{-4}~~ ≥ 10^{-4} to < 10^{-3}
4	4	~~<10^{-4}~~ ≥ 10^{-5} to < 10^{-4}
	~~—~~	~~<10^{-5}~~

E.4.2 Safety Integrity Level (SIL) Assessment ~~Assignment or Availability Value~~

In accordance with ANSI/ISA 61511-1, a necessary step in SIS design is to ~~set~~ determine a target SIL ~~or availability~~ and probability of failure on demand ~~value target for system design~~. The system is assigned as a SIL-1, SIL-2, ~~or~~ SIL-3, or SIL-4 system, with SIL-~~3~~4 being the most robust and ~~most~~ reliable and SIL-1 being the least. ~~Associated with each SIL is a minimum performance requirement, that is, a minimum of 90 % availability for SIL-1, a minimum of 99 % availability for SIL-2, and a minimum of 99.9 % availability for a SIL-3 system.~~ The determination of target SIL for a given system is dependent upon the risk associated with the hazard that the system is protecting against, that is, the likelihood of the initiating and contributing events, the magnitude of the consequences, and the credit that can be taken for other safeguards. The SIL assignment should be performed by a multidisciplinary team.

The acceptability criterion for HIPS performance is expressed in terms of the SIL level, which corresponds to a ~~level of system availability~~ probability of failure on demand (i.e. the probability that the system will not work properly when needed). Each case should be examined individually to determine the appropriate response. The selected SIL for a given system is dependent upon a number of factors, including the following:

a. likelihood of an initiating event placing a demand on the HIPS~~ in the first place (i.e. the likelihood of getting a situation that requires proper action from the HIPS in order to prevent a negative consequence)~~,

b. consequences of a failure of the HIPS, given that a demand has been placed on it,

c. risk tolerance of the user,

d. requirements from local jurisdictional authorities.

~~In the large majority of cases for HIPS, the result of the hazard analysis is either a SIL-2 system (requiring a minimum of 99 % availability) or a SIL-3 system (requiring a minimum of 99.9 % availability).~~

E.4.3 Conceptual Proposal of HIPS Configuration

After a target SIL ~~or availability~~ and probability of failure on demand ~~value~~ ~~has~~ have been ~~assigned~~ determined, a base case HIPS configuration should be devised, with the intention of arriving at a system configuration that meets the ~~availability~~ probability of failure on demand requirement associated with the assigned SIL. At this point, a base case maintenance/testing interval for the individual components of the HIPS should be decided as well. The base case configuration and test data then serve as the basis for the next step in the work process, the Safety Integrity Level (SIL) ~~analysis~~verification, which includes evaluating the system performance and establishing test intervals for the proposed configuration.

E.4.4 HIPS Safety Integrity Level (SIL) ~~Analysis~~ Verification

The purpose of the HIPS Safety Integrity Level (SIL) ~~Analysis~~ verification is to evaluate the system performance of the proposed configuration. The Safety Integrity Level (SIL) should utilize standard techniques, such as fault tree analysis (see ISA-TR84.00.02). In addition to considering the integrity of the hardware, which is addressed in part by suitable scope and frequency of testing, the potential for human error and other sources of systematic failures throughout the system lifecycle should also be considered. The result produced is compared against the performance requirement associated with the assigned SIL to determine if the proposed system is acceptable. If the proposed system does not meet the performance requirement, then it is necessary to modify the system configuration.

~~Careful consideration should also be given in the system design to the calculated rate of nuisance failures. Nuisance trips can be costly and also increase the risk that operators might circumvent the shutdown systems. The potential for nuisance failures can be reduced by including functions such as voting logic and similar techniques to make the application more robust to spurious failures. These provisions can decrease the required testing interval.~~

E.5 Test Intervals for HIPS

~~Faults may occur that prevent the HIPS from functioning as designed. Some faults may be immediately detected (e.g., the final element of a HIPS to cut tower reboiler steam supply spuriously closes resulting in a process shutdown and alarms). Other faults faults may not be detectable without specific proof testing. Periodic proof testing of the HIPS is performed to identify these undetected faults. Requirements for proof testing are found in the relevant SIS standards (e.g., IEC 61511). The proof test interval is a factor in the HIPS Safety Integrity Level (SIL) Analysis verification. Proof testing must be performed as frequently as specified in HIPS design basis to maintain the required SIL-level of the HIPS.~~

Failures can occur in HIPS during operation. Failures which are not detected prior to a demand can lead to a failure of the HIPS to bring the process to a safe state. Failures can be either immediately detected, where the failures is revealed to operations, or undetected. The undetected failures can be detected through diagnostics, proof testing, or preventive maintenance. Safety Integrity Level (SIL) calculations estimate how often the diagnostics, proof testing and preventive maintenance need to be performed. Requirements are found in the relevant SIS standards (see Table E.1). Other considerations such as actual performance

This document is not an API Standard; it is under consideration within an API technical committee but has not received all approvals required to become an API Standard. It shall not be reproduced or circulated or quoted, in whole or in part, outside of API committee activities except with the approval of the Chairman of the committee having jurisdiction and staff of the API Standards Dept. Copyright API. All rights reserved.

records, manufacturers manuals, and safety manuals should be considered also when determining the tasks and frequency of the testing and maintenance.

The designer considering including a HIPS in the facility overpressure protection system should consider the impact of required proof testing on the design and feasibility of the HIPS including:

- Does the frequency and duration of the HIPS testing and/or maintenance render the HIPS unavailable for an unacceptable duration ~~(i.e., can the required availability still be met when considering unavailability for proof testing)~~? Does the overpressure protection design require alternative protection during HIPS testing and/or maintenance or does the process need to be shut down?

- Will the required proof test interval in relation to the process unit shutdown frequency allow for testing during process unit shutdowns or does the required proof test interval drive the need for on-line testing of the HIPS?

- Are facilities to allow on-line proof testing of the HIPS provided in the design (e.g., parallel systems, bypasses, built-in redundancy)? Do the parallel systems and/or bypasses required for proof testing introduce unacceptable operational risks and/or system expense?

E.6 Documentation

The Safety Requirements Specification (SRS) is the controlling document for design, verification, and validation of the HIPS in accordance with the project requirements and specifications and the basis for HIPS performance monitoring and follow-up during the operating lifetime. The safety requirements specification should meet the requirements of IEC 61511.

E.8 Additional Source Material

Additional source material can be found in Bibliographic Items [4], [17], [18], [40], [44], [45], [88], [89], [92], [NEW-1], [NEW-2], [NEW-3], [NEW-4] and [NEW-5].

LIST OF REFERENCES IN API 521 RELATED TO ANNEX E

7th Ed. Ref	Updated Entry for 2023
[4]	[4] API Standard 17O, *Standard for Subsea High Integrity Pressure Protection Systems (HIPPS)*
[17]	[17] ASME *BPVC, Section VIII: Rules for Construction of Pressure Vessels*
[18]	[18] ASME B31 *Code for Pressure Piping*, B31.3, *Process Piping*
[40]	[40] CCPS, *Guidelines for Engineering Design for Process Safety 2ed.*, 2012, ISBN 9780470767726
[44]	[44] CCPS, *Guidelines for Safe Automation of Chemical Processes 2ed.*, 2012, ISBN 9781118949498
[45]	[45] CCPS, *Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis*, 2013, ISBN 9781118777930
[88]	[88] IEC 61508 (all parts) 8, *Functional safety of electrical/electronic/programmable electronic safety-related systems*
[89]	[89] IEC 61511 (all parts), *Functional safety—Safety instrumented systems for the process industry sector*
[92]	[92] ISA TR84.00.02*, Guidelines for the Implementation of ANSI/ISA-61511-1:2018*, 2020.
NEW-1	[Annex E NEW 1] European Commission, *Pressure* ~~Energy~~ Equipment *Directive. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the Harmonisation of the Laws of the Member States Relating to the Making Available on the Market of Pressure Equipment*; European Commission: Brussels, Belgium, 2014.
NEW-2	[Annex E NEW 2] European Committee for Standardization, *EN 764-7:2002, Pressure Equipment – Part 7: Safety systems for unfired pressure equipment,* 2002.
NEW-3	[Annex E NEW 3] ASME *BPVC, Section XIII: Rules for Overpressure Protection*
NEW-4	[Annex E NEW 4] API RP 14C, *Analysis, Design, Installation, and Testing of Safety Systems for Offshore Production Facilities*
NEW-5	[Annex E NEW 5] IOGP Report 443, *High Integrity Protection Systems – Recommended Practice*
NEW-6	[Annex E NEW 6] API Recommended Practice 17V, *Recommended Practice for Analysis, Design, Installation, and Testing of Safety Systems for Subsea Applications*

Items in 7th Edition to REMOVE

~~[52] DIN V 19250, Control Technology; Fundamental Safety Aspects to Be Considered for Measurement and Control Equipment, Deutsches Institut für Normung e. V. (German Institute for Standardization), Berlin~~

~~[91] ISA 84.01 9, Application of Safety Instrumented Systems for the Process Industries~~

~~[92] ISA TR84.02, Functional Safety: Safety Instrumented Systems for the Process Industry Sector—Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004, IEC 61511-2 Mod~~

~~[99] K. A. Kimberly A. and A. E. Summers, “Are Your Instrumented Safety Systems Up to Standard?” Chemical Engineering Progress, Volume 94, Number 11, November 1998, pp. 55–58~~

~~[120] D. F. Montague and J. J. Rooney, Trade-off Risks: Addressing the Tension between Reliability and Safety, International Conference and Workshop on Reliability and Risk Management, San Antonio, Texas, 1998~~

~~[121] M. D. Moosemiller and W. H. Brown, Finding an Appropriate Level of Safeguards, International Conference and Workshop on Risk Analysis in Process Safety, Atlanta, GA, 1997~~

~~[133] OSHA 29 CFR 1910.119 13, Process Safety Management of Highly Hazardous Chemicals~~