International Association of Oil & Gas Producers

REPORT 828 | OCTOBER 2026

Process Safety in Design (PSiD)



Acknowledgements

This Report was authored by the Process Safety in Design Expert Group, part of the Process Safety Subcommittee of IOGP's Safety Committee.

Front cover photography used with permission courtesy of
© Patamaporn Umnahanant/iStockphoto and © Herdik Herlambang/iStockphoto

About

This Report provides guidance to those working on design activities ranging from major capital projects to minor modifications. Firmly based on process safety event data reported to IOGP, this Report highlights a set of Process Safety in Design (PSiD) insights which illustrate some of the more common design pitfalls and opportunities. The specific PSiD insights are framed within a set of overarching Process Safety in Design principles. The intent of this Report is to provide greater line of sight to the learning available within IOGP process safety data and enrich the process safety dialogue within local design teams.

Feedback

IOGP welcomes feedback on our reports: publications@iogp.org

Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained in this publication and any associated material, neither IOGP nor any of its Members past present or future warrants its accuracy or will, regardless of its or their negligence, assume liability for any foreseeable or unforeseeable use made thereof, which liability is hereby excluded. Consequently, such use is at the recipient's own risk on the basis that any use by the recipient constitutes agreement to the terms of this disclaimer. The recipient is obliged to inform any subsequent recipient of such terms.

Please note that this publication and any associated material is provided for informational purposes and adoption of any of its recommendations is at the discretion of the user. Except as explicitly stated otherwise, this publication must not be considered as a substitute for government policies or decisions or reference to the relevant legislation relating to information contained in it.

Where the publication contains a statement that it is to be used as an industry standard, IOGP and its Members past, present, and future expressly disclaim all liability in respect of all claims, losses or damages arising from the use or application of the information contained in this publication in any industrial application.

Any reference to third party names is for appropriate acknowledgement of their ownership and does not constitute a sponsorship or endorsement.

Copyright notice

This publication and the contents of these pages are © International Association of Oil & Gas Producers™ ("IOGP™"). Permission is given to reproduce, quote from, republish, redistribute, and recommunicate this publication in whole or in part for purposes without independent economic value and provided that (i) International Association of Oil & Gas Producers is always acknowledged as the source, together with the words "© International Association of Oil & Gas Producers™ ("IOGP™"), and (ii) any acknowledgments of other sources as may appear in this publication, in respect of such material, are included unaltered. All other rights are reserved.

These Terms and Conditions shall be governed by and construed in accordance with the laws of England and Wales. Disputes arising here from shall be exclusively subject to the jurisdiction of the courts of England and Wales.

REPORT 828 | OCTOBER 2026

Process Safety in Design (PSiD)

Revision history

VERSION	DATE	AMENDMENTS
1.0	October 2026	First release

Contents

Introduction 5

1. Process safety in design 6

2. Process safety in design principles 9

2.1 We systematically identify hazards and reduce risk 10
- 2.1.1. Using relevant techniques to identify hazards and assess risk 10
- 2.1.2. Applying Inherently Safer Design (ISD) and the hierarchy of controls 10
- 2.1.3. Making design decisions informed by the whole lifecycle 11
- 2.1.4. Tips for Leaders 11
- 2.1.5. Implementation guides/resources: 12

2.2 We follow standards and design processes 12
- 2.2.1. Applying industry good practice 12
- 2.2.2. Identifying, reviewing, and communicating change 13
- 2.2.3. Performing activities at the right time, with competent people, using up-to-date information, and a clear design basis 14
- 2.2.4. Conducting systematic assurance processes 15
- 2.2.5. Tips for Leaders 15
- 2.2.6. Implementation guides/resources 15

2.3 We design for ease of use 16
- 2.3.1. Understanding how a design will operate and be maintained in practice 16
- 2.3.2. Providing hardware that is easy to use and supports how work is actually performed 16
- 2.3.3. Making designs more tolerant of errors and less prone to workarounds 17
- 2.3.4. Tips for Leaders 17
- 2.3.5. Implementation guides/resources 18

2.4 We understand the full range of operation conditions and modes 18
- 2.4.1. Establishing design and operating limits for parameters that could lead to a hazardous release 18
- 2.4.2. Understanding both normal and abnormal operating modes 18
- 2.4.3. Tips for Leaders 19

2.5 We provide diverse and reliable prevention and mitigation barriers 19
- 2.5.1. Ensuring expectations placed on human performance are realistic and that critical tasks can be performed reliably 19
- 2.5.2. Handing over barriers built, installed, and documented in accordance with the design intent 19
- 2.5.3. Creating reliable barriers by understanding and managing their failure modes and limitations 20
- 2.5.4. Tips for Leaders 20
- 2.5.5. Implementation guides/resources 21

3. PSiD development and data validation 22

3.1 Mapping of Insights to PSEs 23

3.2 Mapping of PSiD Principles to Insights 24

4. Implementing Process Safety in Design 25

Introduction

Process Safety Event (PSE) data reported to IOGP provides a valuable resource for understanding the types of PSEs that most commonly occur in upstream oil and gas operations, enabling companies to more effectively target their risk reduction efforts. To assist this, IOGP produces supporting tools and publications for supporting Member Companies and beyond. For example, in 2020, IOGP published the IOGP Report 638 - *Process Safety Fundamentals* (PSF) based on analysis of incident data and designed to support those working at the front line of operations, maintenance, and on wells teams.

Further adding to the suite of tools aimed at reducing future process safety events, Process Safety in Design (PSiD) principles and insights have been developed to support companies during design activities ranging from major capital projects to minor modifications.

IOGP estimate that 20%-30% of Tier 1 process safety events have a notable design component and that there are likely many more where deeper analysis could reveal an underlying design aspect or opportunity. In the annual quality assurance exercise for the 2025 reported Tier 1 Process Safety Events, the team identified 60 out of 187 events (approximately 30%) that had a design component (see IOGP Report 2025p - *IOGP Safety performance indicators – Process safety events – 2025 data* – Section 6.1).

The PSiD principles and insights seek to provide greater line of sight to where design issues have contributed to reported PSEs, or to where better design could have avoided a PSE or made it less likely/severe. The intent of the IOGP PSiD principles and insights is not to provide a design manual, but to increase awareness of common design pitfalls and opportunities that are visible from the broad IOGP PSE database. It is hoped that making these insights more available at the "front line of design" will enrich the process safety dialogue amongst design teams and enhance process safety related decision making.

PSiD does not seek to be an exhaustive guide to process safety in design which is addressed by numerous existing industry standards and other publications, some of which are referenced in this document. Rather, it focuses on highlighting some of the more common design issues that still occur despite the wealth of standards and other publications.

The PSiD principles and insights are primarily a data driven resource. The selected PSiD principles were validated against 5 years of IOGP Tier 1 process safety event submissions, with the results of the validation exercise set out in Section 3.

1. Process safety in design

The PSiD principles and insights are intended for use in a broad range of design settings, ranging from major capital projects to small site-based projects and modifications. They can be applied throughout the design phases, from concept selection to detailed design and commissioning where errors can potentially occur that are only revealed years later.

5 Process Safety in Design Principles - application of which reduces the likelihood of future process safety events (PSEs).

The five principles (see Figure 1) underpin the importance of maintaining design integrity throughout the design process and beyond: ensuring that design processes are in place to enable the right design intent to be established and delivered, building on a thorough understanding of the hazards, and delivering a user-friendly system which will work reliably throughout the operations phase. The PSiD principles are illustrated within three broad themes rather than a formal sequence, with each being important to enable delivery of a safe design.

These are overarching principles selected based on IOGP Member Company data and experience, with supporting bullet points for additional detail.

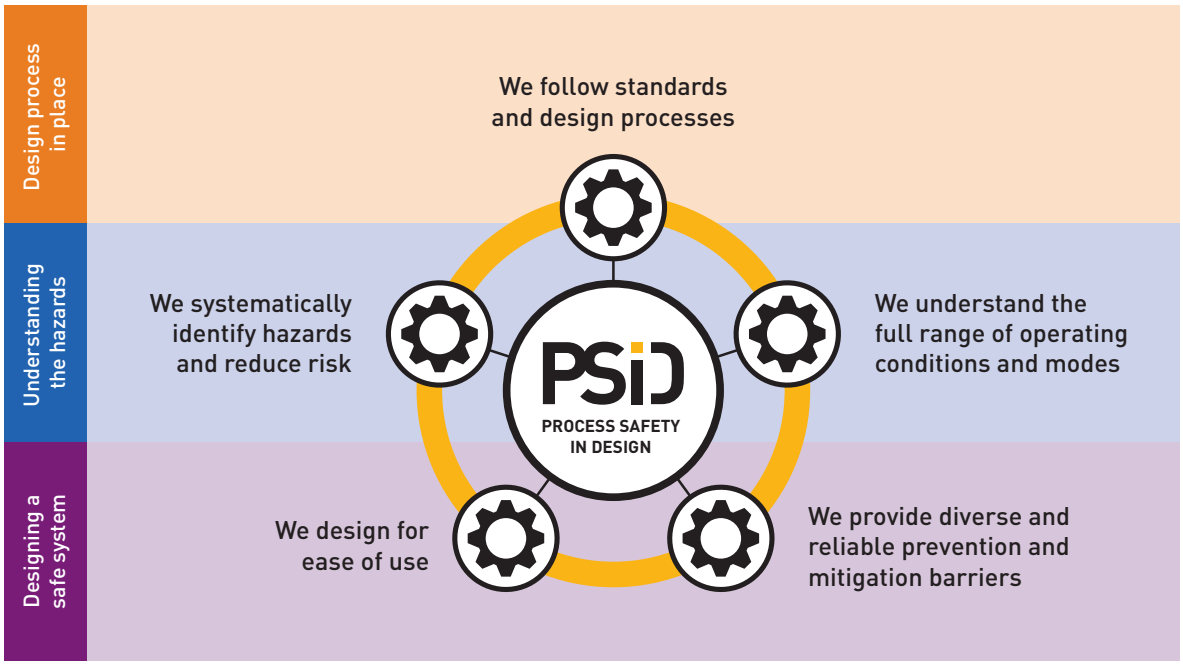


Figure 1 – Process safety in design principles

The supporting narrative sets out the intent and background to each of the 5 PSiD principles, together with tips for leaders.

Tips for leaders are examples of ways that leaders (e.g., facility managers, project managers, contract owners) can behave to promote the application of PSiD principles in their projects and emphasize their significance and priority.

PSiD Insights - Database of insights that PSE data and experience indicate have more commonly either led to design related PSEs or present opportunities to make PSEs less likely/severe. The database is housed on the IOGP website and Figure 2 shows a typical screenshot.

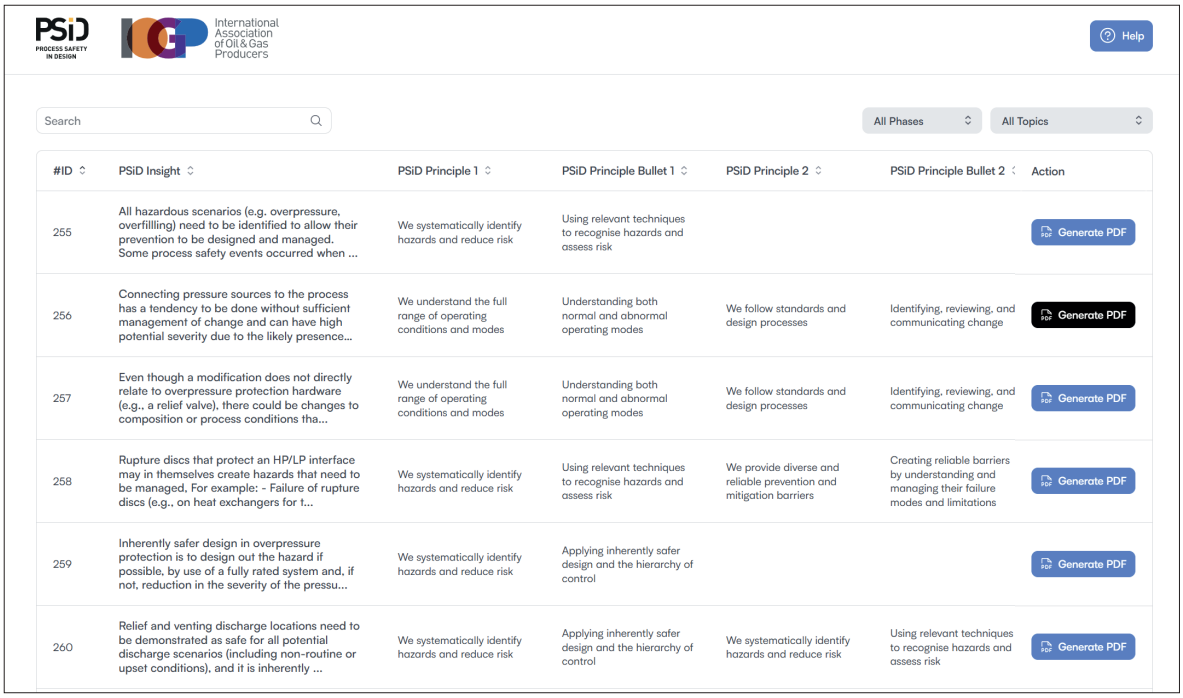


Figure 2 – Example extract from PSiD Insights database

Each numbered PSiD insight is listed together with one or two relevant PSiD principles (and supporting bullets). The most common project phase for application of the insight is listed and, if the screen is scrolled to the right, the associated technical topics.

This tool is intended for use across each engineering design discipline at a working level. To support focused application, insights can be filtered by PSiD principle, technical topic, and project phase, as well as by free text search. To further support users, a one-page worksheet (pdf) can be produced for each insight (see Figure 3). This provides full information for the insight as well as links to process safety event summaries on the IOGP data website that can be used to support discussion.

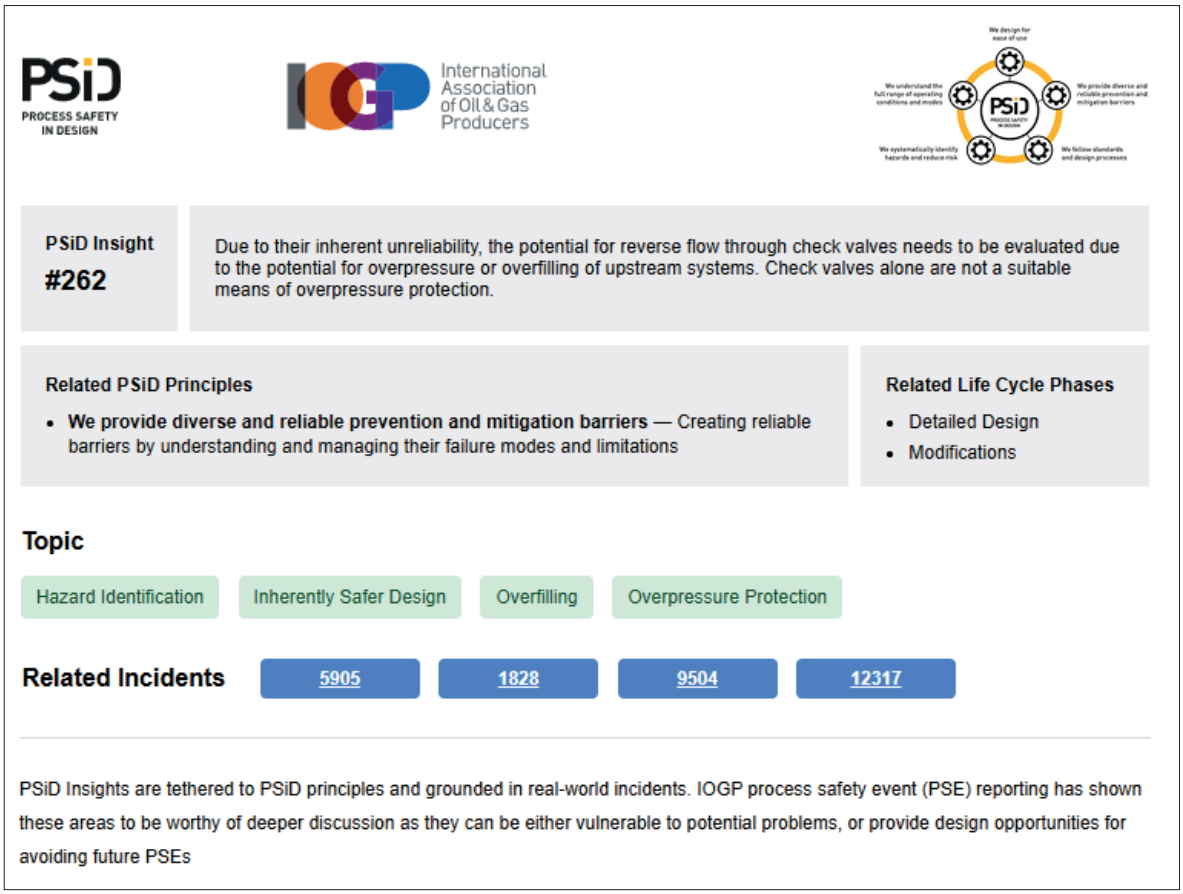


Figure 3 – Example PSiD Insight worksheet

2. Process safety in design principles

We systematically identify hazards and reduce risk

- We use relevant techniques to identify hazards and assess risk.
- We apply inherently safer design and the hierarchy of controls.
- We make design decisions informed by the whole lifecycle.

We follow standards and design processes

- We apply industry good practice.
- We identify, review, and communicate change.
- We are competent and perform activities at the right time, using up-to-date information, and a clear design basis.
- We conduct systematic assurance processes.

We design for ease of use

- We understand how a design will operate and be maintained in practice.
- We provide hardware that is easy to use and supports how work is actually performed.
- We make designs more tolerant of errors and less prone to workarounds.

We understand the full range of operating conditions and modes

- We establish design and operating limits for parameters that could lead to a hazardous release.
- We understand both normal and abnormal operating modes.

We provide diverse and reliable prevention and mitigation barriers

- We make sure that human performance expectations are realistic and that critical tasks can be performed reliably.
- We handover barriers built, installed, and documented in accordance with the design intent.
- We create reliable barriers by understanding and managing their failure modes and limitations.

2.1 We systematically identify hazards and reduce risk

2.1.1. Using relevant techniques to identify hazards and assess risk

Identifying hazards is a vital foundation for achieving good process safety performance, enabling potential consequences and risk to be assessed and appropriate barriers to be designed. Lack of hazard identification and understanding is a consistent contributing factor to process safety events (PSE) reported to IOGP.

Given the complexity of systems that are designed in the oil and gas industry, an effective hazard identification process should be systematic and thorough so that important hazardous scenarios are not missed. Within the context of the overarching industry risk management framework ISO 31000:2018 - Risk management — Guidelines, choosing the right hazard identification technique and applying it at the right time, together with appropriate personnel to conduct and lead the analysis, are important for success.

No single hazard identification technique can be applied across all design phases and so a staged hazard identification approach is normally applied, with earlier assessments often being revisited as design maturity increases. For process excursions, techniques such as Layer of Protection Analysis (LOPA) can be used to assess whether, given the severity of the potential event, there are sufficient barriers (or layers of protection). Many companies also find the use of bowtie diagrams useful for visualizing the management of risk.

Hazard identification should occur early in the design process to maximize the opportunity to manage the hazards. If hazard identification is carried out too late, the opportunity to design inherently safer risk reduction measures, and those better placed in the hierarchy of controls, may have already passed.

Systems involving new technology and less familiar hazards present a particular challenge and can warrant the involvement of specialists and more detailed techniques.

2.1.2. Applying Inherently Safer Design (ISD) and the hierarchy of controls

Application of Inherently Safer Design (ISD) is an opportunity to eliminate hazards or reduce them at source, particularly during earlier project stages and most notably in concept selection. ISD application contrasts with an approach where barriers (consisting of equipment and procedures) are added to manage hazards. Added barriers need to be sustained over the lifetime of the plant, have their own maintenance and testing requirements, and invariably have some potential for failure. ISD features of the design are typically permanent and inseparable from the design, need less or no specific maintenance, and normally cannot be reversed.

Potential ISD benefits include:

- greater uptime, e.g., a system that is fully rated for the maximum pressure compared to reliance on instrumented protective layers and relief systems, both of which can fail, causing downtime
- lower operating costs
- simpler design, with less equipment and smaller hazardous inventories
- reduced staffing and intervention

Reducing exposure of people to hazards is a powerful method of applying ISD, with some concepts being particularly aligned with this goal (e.g., subsea developments, unattended or remote operation, or a bridge-linked platform with separate accommodation jacket). Additionally, at a system design level, avoiding direct interaction with the plant in a way that avoids placing people in the line of fire, or potentially hazardous areas, is an important design driver (e.g., online analysis rather than manual sampling).

Although applicable throughout the design process, the opportunity to incorporate inherently safer features in a design is normally greater at the start of the design process and in greenfield projects. Later in the design process, and in brownfield projects, it can be more difficult and costly to incorporate inherently safer design.

When selecting barriers, the hierarchy of controls approach can be applied throughout the project phases and in both greenfield and brownfield projects. This approach recognizes that engineering barriers typically have greater effectiveness than administrative barriers. Additionally, within the engineering barrier category, passive barriers typically have better reliability than active barriers which have a greater number of failure modes, many of which can remain hidden until a demand is placed on the safety system.

2.1.3. Making design decisions informed by the whole lifecycle

Design decisions should be informed not only by Capital Expenditure (CapEx) considerations but also by full lifecycle implications for safety, operability, maintainability, reliability, and operating costs.

CapEx will often be a key factor in project decision making, however, cost input to decision making should be based on full lifecycle cost evaluation and not solely on CapEx. For example, selecting a low-cost construction material that requires chemical treatment throughout the operating lifecycle can have much higher lifecycle costs when the cost of chemicals, as well as oversight and maintenance of chemical injection systems, is accounted for. It will also be more vulnerable to failure and potential incidents for its whole operating life, with consequential risk and cost.

Additionally, hazards can change during the lifecycle, such as reducing reservoir pressure or later life production fluid souring. Evaluation of the full lifecycle hazard profile enables the most informed design decision making.

2.1.4. Tips for Leaders

- Encourage realistic schedules for hazard identification studies and support teams if they genuinely need more time to complete an effective review.
- Promote good risk decision making by asking the design team to present an open and transparent description of the residual risks to be managed in operations.
- Be balanced in your approach to recommendations; It's fine to push back where appropriate but be equally energetic in your support for good recommendations.
- Champion a culture of learning by asking for examples of incidents from which design lessons have been incorporated.

2.1.5. Implementation guides/resources:

Center for Chemical Process Safety (CCPS). *Guidelines for Engineering Design for Process Safety*. 2012.

Center for Chemical Process Safety (CCPS). *Guidelines for Integrating Process Safety into Engineering Projects*. 2018.

ISO 17776:2016 - Petroleum and natural gas industries - Offshore production installations — Major accident hazard management during the design of new installations

ISO 13702:2024 - Oil and gas industries - Control and mitigation of fires and explosions on offshore production installations - Requirements and guidelines

IChemE, *Applying process safety during concept select phase of a project*. 2020.

Norsok S-001 - Technical safety. 2020.

API RP 14J – Recommended practice for design and hazard analysis for offshore production facilities. 2001.

IEC 61882:2016 Hazard and operability studies (HAZOP studies) – Application guide.

Energy Institute. *Guidance on applying inherent safety in design: Reducing process safety hazards whilst optimising CAPEX and OPEX*. EI3254, 2nd edition. 2014.

Occupational Safety and Health Administration (OSHA). *Identifying Hazard Control Options: The Hierarchy of Controls* https://www.osha.gov/sites/default/files/Hierarchy_of_Controls_02.01.23_form_508_2.pdf

2.2 We follow standards and design processes

2.2.1. Applying industry good practice

Many industry codes, standards, and recommended practices are routinely used in the design of facilities in the oil and gas industry. These documents play a primary role in establishing and enhancing industry good practice and enabling industry standardization. Some codes and standards are mandated by regulation, but application of many relies on companies opting to do so.

These documents also serve to capture industry lessons that have emerged from process safety (and other) incidents, although the speed at which they do this is limited by the need for revisions to be carefully developed, reviewed, and accepted. It is therefore good practice for projects to proactively maintain awareness of lessons from relevant recent incidents.

Beyond this group of formal documents, a range of books and articles provide an additional source of shared learnings.

Application of industry good practice is a fundamental building block of managing process safety during the design process. Mature practice is available which covers both the overall design hazard management process, as well as more specific content on individual barriers such as overpressure protection and safety instrumented systems. IOGP maintains a list

of Operator Key Standards at https://data.iogp.org/Standards. However, application of industry good practice alone is not always sufficient to fully address a hazard, and specific evaluation is often appropriate to develop a hazard management approach.

Many companies supplement industry documents with a set of internal practices. For example, some companies have internal processes that set requirements for which design related activities are performed and their appropriate timing, what data or information needs to be in place to enable the activity to be performed successfully, and the minimum level of competence of those leading and participating in the activity.

Whichever combination of external and internal codes, standards, and recommended practices is selected for a given project, it is important for them to be applied systematically and consistently. A key feature of this is that deviations from a company's requirements undergo a governance process embedded in the company's management system. This governance process includes formal documentation and justification of proposed deviations, review by competent subject matter experts, and a decision made by an accountable and relevant senior person. It is important that the process includes a documented assessment of the impact on hazards and risk for each deviation.

It can be challenging for engineering practice to cover every potential situation that might arise, so having some deviations can be reasonable. However, proposed deviations should be challenged to verify that the circumstances are so unusual that departure from the normal approach is truly warranted and defendable. Companies are advised to be wary of deviations where the proposed justifying logic could be applied to a broad range of cases; these are typically challenges to the requirement itself and are less likely to be defendable as deviations.

2.2.2. Identifying, reviewing, and communicating change

Change management is a key part of process safety in operations but is also important during the design process. Design, by its nature, involves the evolution of ideas, with assumptions and decisions made at an early stage of a project being subject to later update.

For change to be successfully managed during the design process, aspects of the design related to process safety should have a clear point (e.g., a specific document revision number) from which a formal change management process is applied. For design aspects related to the Piping and Instrumentation Diagrams (P&IDs), this trigger point (e.g., a formal document revision) is typically set around the Hazard and Operability (HAZOP) study. Before the HAZOP study, changes to the process design can be made more freely as they will be evaluated during HAZOP. However, changes made to implement HAZOP recommendations, and any other subsequent changes, should be addressed by the formal change management process. For design aspects that are not subject to HAZOP, but that have a process safety function (e.g., gas detector layout, bunding and civil design affecting liquid spill management, structural integrity), a different point of application of change management is typically appropriate.

2.2.3. Performing activities at the right time, with competent people, using up-to-date information, and a clear design basis

Establishing and preserving a clear basis for design is a vital foundation for projects of any size. For larger projects, this is normally formally agreed in a Basis of Design (BoD) document. It provides a shared understanding of project objectives and boundaries amongst key stakeholders, minimizing the potential for misunderstanding. The BoD content unpins many of the activities and decision making relevant to process safety. For smaller projects, this remains a key step although the way in which it is documented is often less formalized.

The design process typically involves performing many interrelated activities and making key decisions according to a project plan and schedule, many of which will influence the future process safety performance of the installed systems. One key factor is for these activities to be performed at the right time in the project's design development when the necessary foundational information and documentation is available. For example, HAZOP performed too early in the design process (when piping and instrumentation diagrams are not sufficiently mature) can reduce the study's ability to identify relevant hazards and can lead to the generation of a large number of recommendations to close out. Conversely, if left too late, the identified hazards will be more difficult to address with desired changes being more costly and potentially unfeasible due to less design flexibility.

Competency of the team and leader that perform process safety related activities is also vital. Some longer-term planning can be required to ensure the availability of the most suitable people.

A strong Terms of Reference (ToR) document or scope document, with relevant leadership approvals or support, for key process safety activities, helps to enable the implementation of activities in a quality manner with the right availability of competent people and relevant up to date documentation.

Various process safety related activities and studies that occur during the design process (such as hazard identification and risk assessment studies covered in Section 2.1) will inevitably generate recommendations or actions. Lack of systematic follow-up and closure of actions can lead to issues being left unresolved and subsequently progressing into operation. These actions should be systematically recorded and managed in a tracking system. The tracking system should normally include the source of each action. Each action's closure should be carried out by relevant and competent personnel with clear evidence of how the action has been addressed. In cases where actions are rejected, it is important that the justification for doing so is recorded, defendable, and signed off by a relevant senior person. It is not recommended to close out actions based on an "agreed intent" to do something. This intent can subsequently be altered or inadvertently overlooked. Action closure is complete only when the agreed intent has been completed and relevant evidence can be referenced.

2.2.4. Conducting systematic assurance processes

Many companies implement a series of assurance reviews during the progress of the design process to confirm that process safety hazards are being suitably managed. These reviews provide an opportunity to involve people with some level of independence from the project to review status with a fresh perspective, and less influenced by the pressures of delivery of the project. Assurance activities should occur throughout the design phases when there is still design flexibility. Assurance in the later project phases is important to verify delivery of the design intent, but it is often too late to influence some key design choices.

One important assurance review is the Pre-Start-Up Safety Review (PSSR). The PSSR includes confirmation that all process safety barriers have been installed as per the design intent, recommendations from safety studies have been completed, and the system is ready for start-up. This includes review of detailed items that can potentially lead to process safety events, e.g., correct failure position of valves, installation of bursting discs in the intended orientation, etc.

2.2.5. Tips for Leaders

- Ask the design team to reflect on whether they have clarity on the design standards to be applied (particularly where requirements are less familiar), and whether the list is aligned with the project's safety goals.
- Discuss the timing of safety studies on the critical path to ensure resulting recommendations can be efficiently implemented.
- Embrace and act on constructive feedback from project design reviews.
- Engage with approvers of deviations seeking clarity on the logic applied and arrange for learning to be fed-forward for future designs.
- Promote the importance of adherence to Management of Change (MOC) processes by encouraging the design team to share lessons from where MOC has failed.

2.2.6. Implementation guides/resources

Center for Chemical Process Safety (CCPS). Guidelines for Integrating Process Safety into Engineering Projects. 2018.

ISO 17776:2016 - Petroleum and natural gas industries - Offshore production installations — Major accident hazard management during the design of new installations.

Energy Institute, Guidance on meeting expectations EI Process safety management framework. EI3276. 2015.

2.3 We design for ease of use

Many process safety event investigations identify human error as an immediate cause of an incident. Whilst this might be true, it offers little risk reduction insight. Dr. Trevor Kletz likened it to saying that all falls are due to gravity.[1] It is much more helpful to understand the underlying conditions that led to the error; and some of the most influential underlying conditions are set during the design process. It is therefore likely that design, as a contributor to human error, is an underestimated factor in process safety event causation.

Good design is based on an understanding that humans sometimes make mistakes, and these are strongly influenced by the design of underlying systems and processes. By understanding the relevant human performance issues, the designer can ensure that those who will operate the plant are set up for success rather than failure by ensuring systems are easy to use and tolerant of error.

IOGP Report 454 - *Human Factors Engineering in Projects* offers recommendations for integrating human factors into the design process.

2.3.1. Understanding how a design will operate and be maintained in practice

Just as hazard identification is a crucial foundation for hazard management, it is important for the designer to understand how the plant will be operated and maintained in practice. This consideration includes understanding the capabilities of those who are going to operate and maintain the plant. Failure to do this can potentially result in unidentified or unresolved issues progressing into operation, leading to future process safety incidents or the need for later modifications to address issues.

Human factors-related activities should involve collaboration with operationally experienced personnel to understand how the design will be used in practice. This involvement should occur sufficiently early in the design process when there is still opportunity to influence it. Review of 3D models is one specific way of beneficially bringing operational experience into the project at a stage when changes are still relatively easy and can provide specific focus on layout and access issues. The timing of the reviews should be performed when the 3D model is sufficiently mature, but early enough to enable observations to be incorporated.

Additionally, the broader range of human performance issues and how they can be appropriately addressed in the design should also be systematically addressed.

2.3.2. Providing hardware that is easy to use and supports how work is actually performed

One of the obstacles to designing easy to use (and, hence safer) systems is that there is sometimes a disconnect in the understanding of how a system will operate between the designers and the future operators. This is sometimes described as "work as imagined" (in the design office) versus "work as done" (how work is actually conducted in operation). Further explanation can be found in IOGP Report 642 - *Learning from normal work*. Designers should acknowledge this potential weakness and make efforts to understand how work will be performed in practice. Early involvement of experienced operations and

[1] Brazier A et al, *Trevor Kletz Compendium*. Elsevier. 2021.

maintenance personnel is one practical enabler for designing equipment and systems that support "work as done."

Identification of critical tasks enables design effort to be focused on areas where prevention of human error will be most effective in reducing risk. Once these tasks are identified, active and regular involvement of experienced operations/maintenance representatives and human performance specialists can help to support a more realistic understanding of "work as done", and to produce a design that is easy to use and reduce the gap against "work as imagined".

2.3.3. Making designs more tolerant of errors and less prone to workarounds

The human performance principles that IOGP has aligned with (see IOGP Report 810 – *Human Performance*), recognize that error is normal and that even well trained, competent people will make mistakes. The principles also point out that context drives behaviour and that mistakes are typically due to underlying conditions and systems. Therefore, during the design process, the reality of future human error during operations and maintenance should be recognized, and systems/equipment should be designed that are error tolerant and error resistant.

One approach is to evaluate if the design is vulnerable to workarounds being established. The inevitable pressures of an operational environment can be a driver for quicker and easier methods to be sought. Sometimes, these shortcuts or workarounds conflict with the process safety design intent. Ensuring that systems are easy and convenient to use will limit the incentive to seek out workarounds. Further explanation on workarounds can be found in IOGP Report 642 - *Learning from normal work*.

It is recommended that formal human factors assessments are conducted at appropriate stages of the design process with the support of human performance specialists (see IOGP Report 454 - *Human Factors Engineering in Projects*), appropriately scaled for the project size, complexity, novelty, and risk. This should be supplemented by enhancing human performance understanding and awareness across the whole design team, so that human performance thinking is included as part of normal everyday design work across the range of engineering disciplines.

2.3.4. Tips for Leaders

- Insist on strong operations and maintenance representatives at appropriate design stages.
- Request briefings on key human performance risk areas and discuss these with the disciplines who can influence them.
- Encourage the design team to showcase where they have applied design standardization and human factors engineering to secure ease of use.
- Ensure the project has access to experienced human performance capability.

2.3.5. Implementation guides/resources

IOGP Report 454 - *Human Factors Engineering in Projects*

IOGP Report 642 - *Learning from normal work*

IOGP Report 810 - *Human Performance*

Energy Institute, *Guidance on human factors safety critical task analysis*. EI3201. 2nd edition. 2020.

ASTM F1166-23 - Standard Practice for Human Engineering Design for Marine Systems, Equipment, and Facilities, 2023.

2.4 We understand the full range of operation conditions and modes

2.4.1. Establishing design and operating limits for parameters that could lead to a hazardous release

Going outside the intended design envelope, both in terms of operational conditions and mode of operation, is another major factor in process safety incidents reported to IOGP.

Operating envelopes that set upper and lower limits for acceptable ranges of operation for each process parameter (e.g., pressure, temperature, level, flow, composition) are needed, where relevant. Setting of operating envelopes starts in the design phase with management of operating envelopes continuing throughout the operating life of the asset. Relevant instrumentation should be included in the design to support the monitoring of operating envelopes and to identify excursions.

Numerous incidents have occurred where the lack of systematic definition of operating envelopes has led to the equipment or system being inadequately specified for the duty it sees in practice. The most common example of this is material selection for systems that will see more challenging process fluids in later field life (e.g., increased water and/or hydrogen sulphide). Additional initial capital cost of more corrosion/erosion resistant materials is often less expensive over the operating life of the plant due to fewer process safety events and lower operating costs. Companies should ensure they evaluate the anticipated operating conditions (including stream compositions) for the full anticipated asset life, as they make material selection decisions. Design assumptions (e.g., feed composition, product specification) that change during the design process can be a root cause of future PSEs and should be systematically managed using a formal management of change process.

2.4.2. Understanding both normal and abnormal operating modes

Unintended or unexpected modes of operation are another regularly observed route to PSEs. As well as potentially causing an operating limit excursion, unforeseen modes of operation are unlikely to have been subject to the relevant hazard identification and risk assessment processes and consequently appropriate barriers are sometimes absent. An important element of the design process is to identify and document all anticipated

modes of operation and complete the corresponding hazard identification and risk evaluation activities. Good documentation, including development of a written operating philosophy, enables those who operate and maintain the plant later to understand the intended operating modes and determine what additional management of change and risk assessment processes are needed if operation outside this is intended. Involvement of experienced operations and maintenance personnel can also assist in identifying less obvious operating activities.

Examples of unanticipated activities that have led to PSEs include:

- draining and sampling from ad-hoc locations
- reverse flow from export pipelines at start-up
- connection of air or nitrogen hoses for purging or pressurization

2.4.3. Tips for Leaders

- Ask your teams to challenge how future operational modes have been anticipated and whether the design is flexible enough to accommodate them.
- Invite the operations team to discuss previous incidents during transient operating modes with the design team.
- Review the operating experience in the design team and arrange further support if needed.

2.5 We provide diverse and reliable prevention and mitigation barriers

2.5.1. Ensuring expectations placed on human performance are realistic and that critical tasks can be performed reliably

It is important to ensure that human tasks within barriers (often termed 'critical tasks') are both feasible and can be performed reliably. This includes evaluation of the operational context, the time available, and other factors which could influence human performance.

2.5.2. Handing over barriers built, installed, and documented in accordance with the design intent

Once the barriers have been selected, the project should deliver a system that is consistent with the design intent. The intended risk reduction can only be sustained if the barriers are maintained and tested throughout their operating life. During the design phase, thorough documentation should be prepared for handover to operations to enable the design intent of the barriers to be fully understood and for them to be managed for their full lifecycle. If not handled with discipline and rigor, handover to operations can result in a significant loss of design integrity during the intense period leading up to start-up (e.g., punch list management, construction deviations, late field changes, etc).

Designers should deliver systems and documentation (e.g., performance standards, testing requirements, failure modes) which enable the health of each barrier to be readily and efficiently monitored. Good practice for many barriers involves automatic collection of barrier health data, where practical, with a dashboard to allow easy oversight (e.g., live data on the health of safety instrumented systems, alarm activation rates, and operating limit excursions).

2.5.3. Creating reliable barriers by understanding and managing their failure modes and limitations

Elimination or substitution of hazards by application of inherently safer design is the starting point for hazard management, but residual risks will remain that need to be managed by barriers (protection layers). The Swiss Cheese model for hazard management illustrates that no barrier is infallible and the importance of being realistic about the level of risk reduction provided by each barrier. It is good practice to incorporate a range of independent barriers including both prevention and mitigation barriers (more information on barriers can be found in IOGP Report 544 - *Standardization of barrier definitions*). The concept of providing a range of barriers, recognizing that each will have some weakness, is sometimes referred to as defense in depth. Many companies find that the use of bowtie diagrams and/or workshops can be helpful in barrier identification, visualization, and health assessment.

As all barriers have the potential to fail, the limitations and failure modes of deployed barriers should be understood to ensure that they are being used in the right way and that only realistic risk reduction expectations are placed on them. Close attention should be given to the independence of barriers to ensure that the risk reduction that the design assumes is delivered in practice. Barriers that share points of potential common cause failure (e.g., power supplies, impulse lines) will often deliver much reduced risk reduction compared to genuinely independent barriers.

2.5.4. Tips for Leaders

- Discuss with the design team the application of ISD and the hierarchy of controls: challenge if they can find solutions higher up the hierarchy. Ask "what would it take to eliminate this hazard?"
- Invite the design team to reflect on how their processes will result in the right barriers in the design to prevent and mitigate major accident events.
- Ask if the design is reliant anywhere on a single barrier.
- Demonstrate leadership commitment by taking time to talk with the team about the importance of barrier reliability and diversity and show a willingness to accept some project disruption to achieve risk reduction. Ask for, and discuss, key examples.

2.5.5. Implementation guides/resources

IOGP Report 544 – *Standardization of barrier definitions*

Energy Institute, *Bow ties in risk management: A concept book for process safety*, EI3368, 2018.

ISO 17776:2016 - Petroleum and natural gas industries - Offshore production installations — Major accident hazard management during the design of new installations

IEC 61511:2026 – Functional safety – Safety instrumented systems for the process industry sector – ALL PARTS

API Std 520 - Sizing, Selection, and Installation of Pressure-relieving Devices, 10th edition, 2020.

API Std 521 – Guide for Pressure-relieving and Depressuring Systems, 7th edition, 2020.

3. PSiD development and data validation

Development of the PSiD principles and insights was conducted by an Expert Group (EG) formed by the IOGP Process Safety Subcommittee (PSSC).

A key aspect during the project was that the PSiD content needed strong roots in the process safety data submitted to IOGP. Consequently, the PSiD principles and insights are supported by IOGP data as well as the wealth of company experience in the EG.

The EG was also aware that the PSE data submitted by companies typically only provides a high-level overview of the PSE causation and potential learnings. Inevitably, the brief PSE descriptions submitted tend to give particular focus to immediate cause and context of the PSE with the design aspects, however valid, being more latent and less well described. Therefore, the EG applied a level of judgement to identify design issues behind them.

PSiD principles and insights broadly took the following development path:

Members of the EG were requested to submit details of recent serious process safety events and process safety related high potential incidents where their investigation indicated a significant causal aspect related to design. An overview of these incidents was consolidated, and a set of common topics was identified.

A set of overarching PSiD principles was identified by the EG. These PSiD principles were updated and validated by mapping to a 5-year history of Tier 1 PSEs reported to IOGP 2019-2023.

For each of the common themes, specific PSiD insights were identified based on process safety event data and member experience.

- The list of PSiD insights was further validated by mapping to a 5-year history of Tier 1 PSEs reported to IOGP 2019-2023. This data mapping exercise enabled identification of further insights which were added.
- The full list of PSiD insights underwent a line-by-line validation exercise with the EG in which each insight was mapped to one or two PSiD principles and assigned an association with each relevant topic to enable filtering by users.
- Each year the PSSC conducts a quality assurance (QA) review of the annual Tier 1 PSE submissions. This review involves an incident-by-incident review of the submitted information by the QA team. The QA reviews conducted in 2024 and 2025 included an additional task to identify which of the incidents gave a significant design insight. The intent going forward is for this to continue as part of the annual process. This is likely to give rise to further PSiD insights being identified which can be added to the online tool.

3.1 Mapping of Insights to PSEs

Review of 985 reported PSEs between 2019 and 2023 (inclusive) indicated that over 30% supported a PSiD insight to some extent, although design was not necessarily cited as the primary concern in all cases. When each of these incidents was assigned a most relevant PSiD principle, the following distribution was seen:

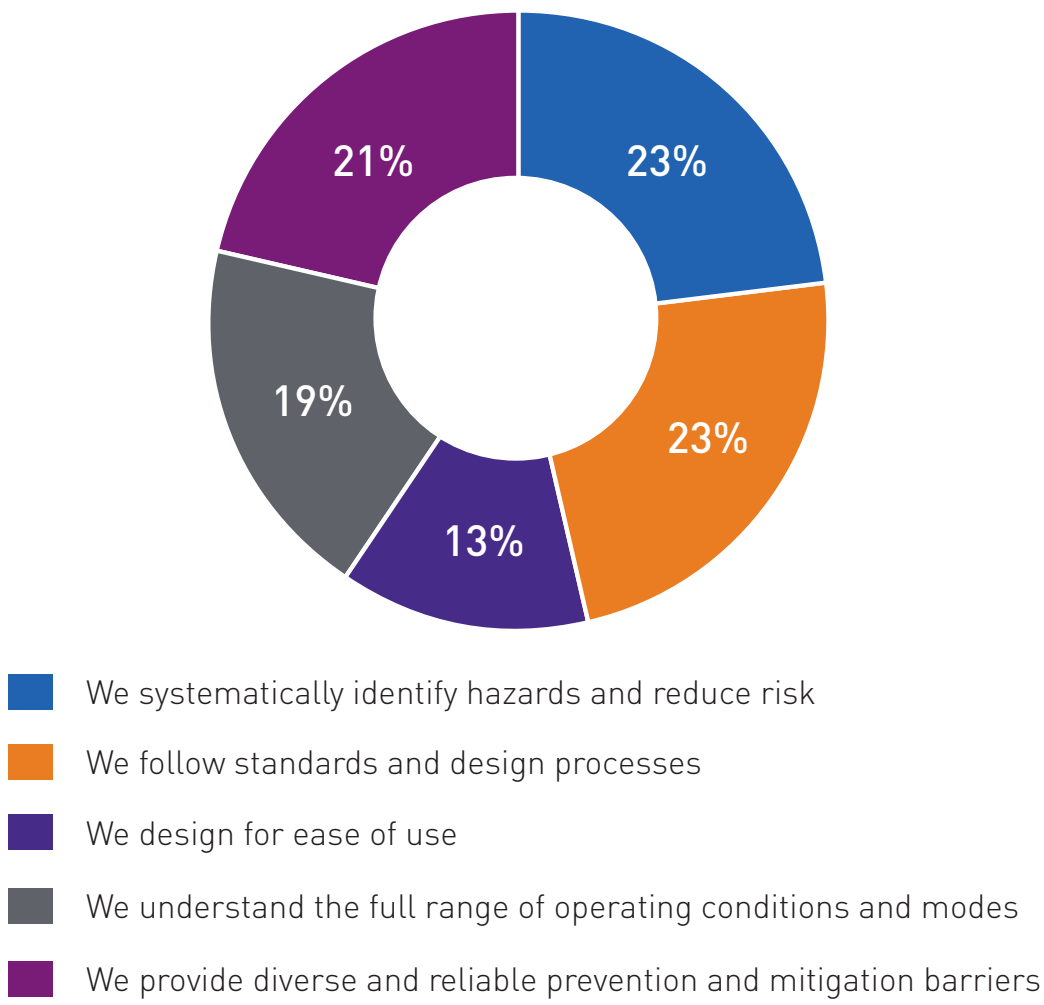


Figure 4 – Allocation of PSiD Principles to PSE Tier 1 2019-2023

3.2 Mapping of PSiD Principles to Insights

When each of the individual PSiD insights were mapped back to a PSiD principle (and by exception a second, if relevant), the following distribution was observed. Together with the linkage of PSiD insights to reported PSEs, this provides confidence that the combination of PSiD principles and insights is firmly rooted in data and provides insight coverage across the range of topics addressed by the PSiD principles.



Figure 5 – Mapping of PSiD Principles to PSiD Insights

4. Implementing Process Safety in Design

IOGP PSiD principles and insights are provided to enable companies to enhance and energize their process safety conversations at the "front line" of design.

PSiD implementation involves engagement of the whole project team, embedding the use of the PSiD principles and insights in a broad range of project activities. PSiD is not intended as an additional add-on activity, but rather to be integrated into existing design activities and workflows, reinforcing and developing their process safety content and strength.

To enable successful implementation, it is recommended that a senior person within the project 's leadership (e.g., engineering manager) should be nominated to act as a champion for integration of the PSiD principles and insights. This nominated individual can be accountable for ensuring the right level of engagement with PSiD across the project team and providing ongoing verification of application.

Corporate leadership and project teams are encouraged to consider how PSiD principles and insights can be used to greatest effect in their own specific context, but the following list offers some examples as a starting point.

Leadership commitment and behaviours – A documented leadership statement can demonstrate the project's commitment to driving excellence in PSiD and integrating the PSiD principles and insights into the project's day-to-day activity set. Further tips on how leadership behaviours can support implementation of PSiD are provided in Section 2 of this document.

Leadership communication – To vocalize the importance of PSiD to the project team across all disciplines. This can be illustrated with process safety incidents in which design was a causal factor, demonstrating how application of the PSiD principles and insights could have avoided the incident.

Maintaining project-wide PSiD dialogue – Presentations at Town Halls and other project meetings can help to maintain the profile of PSiD and to support understanding within the project team of its value. Up-to-date posters in the project office can be a powerful communication tool, including impactful relevant images that can be displayed at strategic positions.

Integration into regular discipline meetings – Regular discipline meetings (particularly at the start of key design activity) provide an excellent opportunity for discussion of selected PSiD insights to discuss and evaluate how they can be applied to the specific project design.

Integration into discipline checklists – Engineering functions often maintain discipline checklists to enable their activities to be thorough and complete. The content of these checklists can be reviewed in the light of the PSiD principles and relevant insights, to further develop and target the checklist content.

PSiD Safety Moments – Use of PSiD insights that are of particular relevance to the project as safety moments in meetings can prompt healthy challenge and discussion.

Integration into project planning – Application of PSiD can be included in project planning to increase its profile and ensure stakeholders are aware of the intent to use PSiD principles and insights.

Incident investigation – PSiD provides a useful reference for investigations of design related process safety events.

Inclusion in training – Project process safety (or other) training activities can include appropriate PSiD material to ensure awareness and understanding of its importance and content.

Developing case studies for discussion – PSiD case studies, based on IOGP reported PSEs (or other industry and company incidents) can provide useful material to prompt deeper thinking about application of PSiD insights within a project's specific context.

PSiD input to assurance and audit activities – PSiD insights can be used selectively to support development of the agenda and content of assurance and/or audit activities to provide focus on relevant areas that PSE data indicates are worthy of deeper review.

Engagement discussions between operator and contractor – Given the importance of both the operator and contractor being committed to the application of PSiD, the principles and insights can be used to supplement engagement discussions to enable alignment of common intent.

Preparation and prework for process hazard analysis (e.g., HAZOP) – Thorough preparation and prework for process hazard analysis studies is important to enhance their effectiveness and efficiency. Consideration of relevant PSiD insights during the prework phase can alert the team to potential problem areas that could benefit from detailed review during the study.

Integration into pre-start up safety reviews – Some of the PSiD insights relate to the importance of delivering the design as intended, ensuring appropriate documentation and providing effective quality control. Review of appropriate PSiD insights can highlight areas that could require particular attention during the pre-start up safety review.

Figure 6 illustrates an example of PSiD focus by project stage. Companies are encouraged to evaluate how best to integrate PSiD into their specific design context.

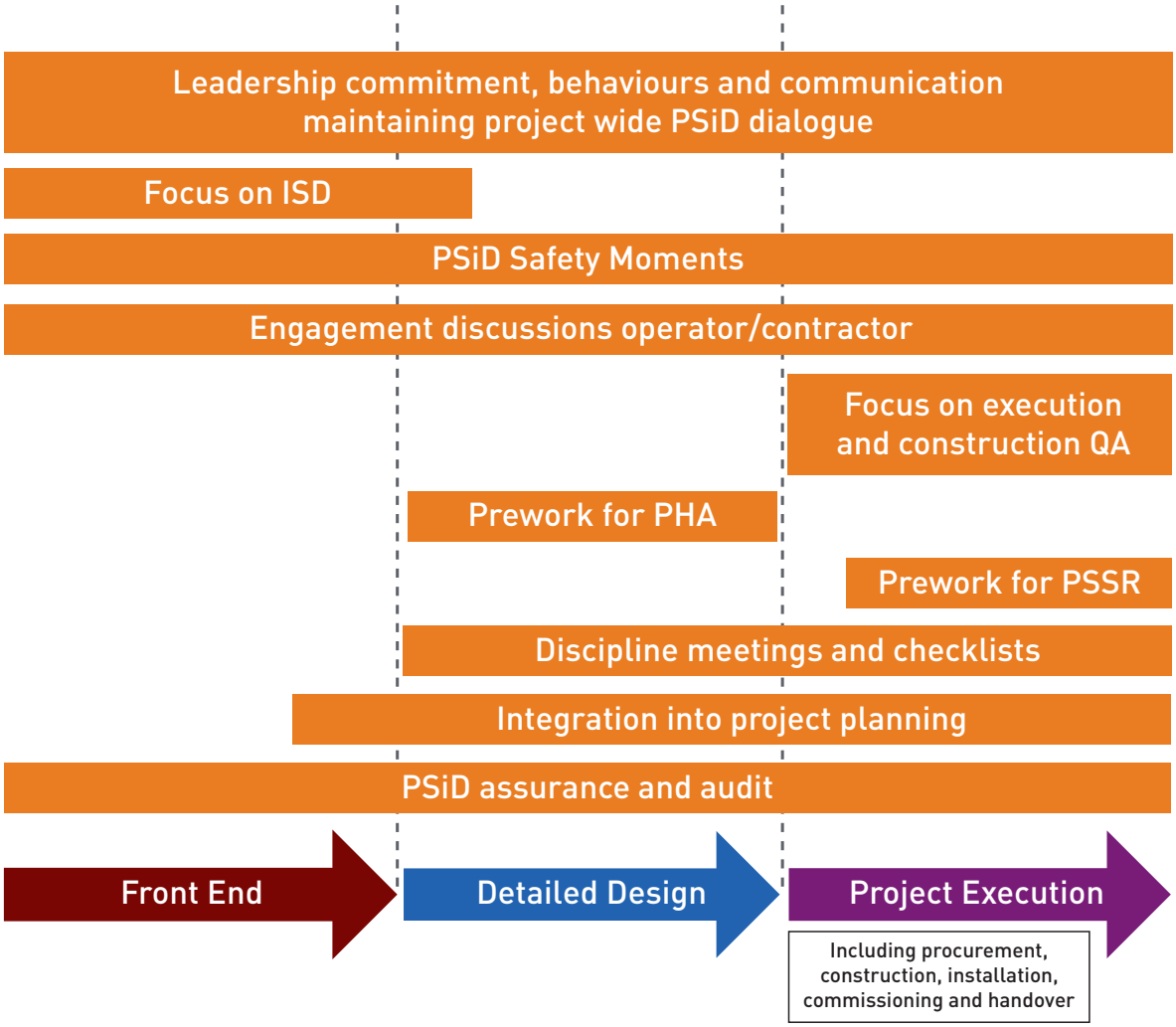


Figure 6 – Example timing of PSiD application

International Association of Oil & Gas Producers

This Report provides guidance to those working on design activities ranging from major capital projects to minor modifications. Firmly based on process safety event data reported to IOGP, this Report highlights a set of Process Safety in Design (PSiD) insights which illustrate some of the more common design pitfalls and opportunities.

The specific PSiD insights are framed within a set of overarching Process Safety in Design principles. The intent of this Report is to provide greater line of sight to the learning available within IOGP process safety data and enrich the process safety dialogue within local design teams.

IOGP Headquarters

3 Moorgate Place, London, EC2R 6EA, United Kingdom
T: +44 20 4570 6879
E: reception@iogp.org

IOGP Europe

T: +32 2 210 94 40
E: reception-europe@iogp.org