HIGH PRESSURE PROTECTION SYSTEM (HIPPS)

TOP 50 QUESTIONS & ANSWERS

admin@instrunexus.com

www.instrunexus.com

INSTRUNEXUS

HIPPS: Top 50 Interview Questions

A comprehensive guide to High Integrity Pressure Protection Systems for professionals.

BAR·G INSTRUNEXUS

What is HIPPS?

A High Integrity Pressure Protection System (HIPPS) is a type of Safety Instrumented System (SIS) designed to prevent over-pressurization of a plant, pipeline, or process system. It provides a barrier between a high-pressure source and a downstream system with a lower pressure rating, shutting off the source of pressure *before* the design pressure is exceeded. This avoids loss of containment and protects personnel, the environment, and assets. It is considered the last line of defense, activating when other control and safety layers have failed.

What is the primary purpose of a HIPPS?

The primary purpose of a HIPPS is to provide a high-integrity, automated, and independent safety barrier to prevent catastrophic over-pressurization of a downstream system.

- It acts as a barrier, isolating a high-pressure (HP) source from an adjoining low-pressure (LP) system.
- It is designed to activate *before* the pressure exceeds the safe operating limits of the LP system, preventing rupture or failure (loss of containment).
- It enhances safety, protects the environment from spills, and safeguards capital assets from damage.
- It is often used in place of, or in addition to, conventional relief systems (like PSVs) where flaring or venting is undesirable or impractical.

What are the main components of a typical HIPPS loop?

A HIPPS loop consists of three main subsystems, following the "sensor-logic solver-final element" architecture of any Safety Instrumented Function (SIF):

- **Initiators (Sensors):** These are the "eyes" of the system.
  - Typically high-integrity pressure transmitters or pressure switches.
  - They are installed with high redundancy, often in a 2-out-of-3 (2oo3) or 1-out-of-2 (1oo2) voting arrangement to ensure reliability and avoid spurious trips.
- **Logic Solver:** This is the "brain" of the system.
  - A high-integrity, certified safety PLC (Programmable Logic Controller) or a solid-state/hard-wired relay system.
  - It receives signals from the sensors, performs the voting logic (e.g., 2oo3), and decides whether to initiate a shutdown.
  - Must meet a specific Safety Integrity Level (SIL).
- **Final Elements:** These are the "hands" of the system that perform the safety action.
  - Typically consist of one or more quick-closing, high-reliability shut-off valves (e.g., ball valves or gate valves).
  - Each valve has its own actuator (hydraulic, pneumatic) and often a solenoid valve (SOV) to control the actuator.
  - Redundancy is common, such as two valves in series (1oo2) to ensure a tight shut-off even if one valve fails to close.

INSTRUNEXUS

When would you use a HIPPS instead of a conventional Pressure Safety Valve (PSV)?

HIPPS is chosen over conventional relief systems (like PSVs or rupture disks) in specific scenarios:

- **Environmental Concerns:** When releasing the process fluid (e.g., toxic gas like H_2S, flammable hydrocarbons) to the atmosphere or a flare system is environmentally unacceptable.

- **Economic Unfeasibility:** When the required relief rate is so large that the flare system, knockout drums, and piping would be impractically large and expensive.
- **Process Reasons:** When releasing the fluid would create secondary hazards, such as hydrate formation (Joule-Thomson effect) or auto-refrigeration that could make pipes brittle.
- **Location Constraints:** On offshore platforms or in urban areas where a large flare is not feasible or safe.
- **Risk Reduction:** When the risk of overpressure is high and the consequences are catastrophic, requiring a more reliable and faster-acting protective layer than a PSV.

What is "SIL" and why is it critical for HIPPS?

SIL stands for Safety Integrity Level. It is a discrete level (1 to 4) for specifying the safety integrity requirements of the safety functions to be allocated to the safety-instrumented systems.

INSTRUNEXUS

- **Definition**: SIL is a measure of risk reduction provided by a Safety Instrumented Function (SIF). A higher SIL level (e.g., SIL 3) provides a greater degree of risk reduction than a lower one (e.g., SIL 1).
- **Criticality for HIPPS:**
    - HIPPS is often the *last line of defense* protecting against a high-consequence event (e.g., vessel rupture).
    - Because it replaces a "passive" device like a PSV, it must have extremely high reliability.
    - Therefore, HIPPS are almost always required to meet SIL 3, and in some rare, extreme-risk cases, SIL 4 (though SIL 4 is more common in nuclear or rail).
    - Meeting a specific SIL level dictates the required system architecture (redundancy), component selection, testing frequency, and management procedures for the entire system lifecycle.

SIL Levels & Probability of Failure on Demand (PFD):

- SIL 1: PFDavg = 10^{-1} to 10^{-2} (Risk Reduction Factor: 10 to 100)
- SIL 2: PFDavg = 10^{-2} to 10^{-3} (Risk Reduction Factor: 100 to 1,000)
- SIL 3: PFDavg = 10^{-3} to 10^{-4} (Risk Reduction Factor: 1,000 to 10,000)
- SIL 4: PFDavg = 10^{-4} to 10^{-5} (Risk Reduction Factor: 10,000 to 100,000)

Explain the 2-out-of-3 (2oo3) voting logic used for HIPPS sensors.

2oo3 (Two-out-of-Three) voting is a common fault-tolerant architecture used for the sensors (pressure transmitters) in a HIPPS.

- How it works: Three independent sensors monitor the same process pressure. The logic solver is programmed to initiate a shutdown *only* if at least two of the three sensors detect a high-pressure condition (i.e., they "vote" for a trip).
- Advantages:
    - Fault Tolerance (Safety): If one sensor fails "dangerously" (e.g., fails to detect a true high pressure), the other two can still vote to trip the system. The system remains safe.
    - Spurious Trip Avoidance (Availability): If one sensor fails "safe" (e.g., provides a false high-pressure reading), it will only cause one "vote." The system will not shut down because the other two sensors read normal pressure. This prevents a false trip, which is crucial for plant availability.
- Diagnostics: The logic solver can compare the readings from all three sensors. If one sensor's reading deviates significantly from the other two, it can flag an alarm for maintenance, allowing the faulty sensor to be repaired online without shutting down the process.

INSTRUNEXUS

What are the key international standards governing HIPPS?

HIPPS design, implementation, and maintenance are governed by the primary standards for functional safety:

- IEC 61508: This is the fundamental, "umbrella" standard for "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems." It covers the entire safety lifecycle for all industries and provides the framework for SIL determination and verification.

- IEC 61511: This is the process industry-specific implementation of IEC 61508, titled "Functional safety – Safety instrumented systems for the process industry sector." This is the primary standard used for designing HIPPS in oil and gas, chemical, and petrochemical plants. It details the safety lifecycle from hazard analysis (HAZOP) to decommissioning.
- API 14C: While a US standard ("Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms"), its principles are widely adopted. It provides guidance on safety system design, including pressure protection.
- ASME B31.8 / B31.4: These standards for gas and liquid pipelines, respectively, may contain sections relevant to overpressure protection, especially for pipeline-specific HIPPS applications.

What is the difference between PFD and PFDavg?

INSTRUNEXUS

Both relate to the reliability of a safety function, but they measure slightly different things:

- PFD (Probability of Failure on Demand): This represents the probability that a safety function will fail to perform its intended function *at the specific moment* a demand occurs. This value is not static; it increases over time as components degrade (e.g., a valve gets stuck).
- PFDavg (Average Probability of Failure on Demand): This is the *average* value of the PFD over the system's proof test interval. Since PFD starts low (just after a test) and increases until the next test, PFDavg provides a more practical metric for SIL verification.
  - When we say a system is SIL 3, we mean its PFDavg is between 10^{-3} and 10^{-4}.
  - The PFDavg is directly influenced by the system's architecture (redundancy), component failure rates (λ_D), and the Proof Test Interval (TI). A shorter test interval results in a lower PFDavg.

What is a "Proof Test" and why is it mandatory for HIPPS?

A Proof Test is a comprehensive, periodic test performed on a safety system (like HIPPS) to reveal *all* undetected "dangerous" failures that may have accumulated since the last test.

- **Purpose**: The primary goal is to find "covert" or "dormant" faults. A HIPPS system sits idle, sometimes for years, and a component could fail (e.g., a valve actuator corrodes, a relay sticks) without anyone knowing. The proof test is the *only* way to find these failures.
- **Mandatory Requirement:**
  - Proof tests are mandated by IEC 61511.
  - The Proof Test Interval (TI) is a critical parameter in the SIL calculation. The entire PFDavg calculation is *based on the assumption* that these tests will be performed at the specified interval (e.g., once every 1, 2, or 5 years).
  - Skipping or delaying a proof test invalidates the SIL rating of the HIPPS, meaning the system can no longer be guaranteed to provide the required level of risk reduction.
- **Scope**: A full proof test must be "as-good-as-new," meaning it should test every component in the loop, from the sensors (by applying a known pressure) to the logic solver and the final elements (by fully stroking the valves).

Explain Partial Stroke Testing (PST). What are its benefits and limitations?

INSTRUNEXUS

Partial Stroke Testing (PST) is a diagnostic test performed on the final element (valves) *while the plant is still online*.

- **How it works**: The logic solver commands the valve to move a small amount (e.g., 10-20% of its full travel) and then returns it to the fully open position. This is done slowly and in a controlled manner so as not to upset the process.
- **Benefits:**
  - Finds Failures Early: PST can detect a high percentage (e.g., 60-80%) of "stuck" failures without requiring a full shutdown. This is a massive operational advantage.
  - Extends Proof Test Interval: By performing frequent PST (e.g., every 3-6 months), you can claim a higher "diagnostic coverage." This can be used in the SIL calculations to justify extending the interval for the much more disruptive *full* proof test (e.g., from 1 year to 3 years).
  - Increases Confidence: It gives operators confidence that the valves are mechanically free and will likely work when needed.
- **Limitations:**

    - Not a Full Test: PST *cannot* detect all failures. It cannot confirm the valve's ability to achieve a "tight shut-off" (seat integrity) or that it can travel the last 10-20% of its stroke.
    - Does NOT Replace Proof Testing: PST is a *supplement* to, not a replacement for, the full proof test. The full proof test must still be done at the (now extended) interval.
    - Risk of Upset: If not designed or executed properly, a PST could accidentally trip the plant or upset the process.

What is a "spurious trip" and how does HIPPS architecture minimize it?

A spurious trip (or "nuisance trip") is an unplanned shutdown of the process caused by the safety system *when no actual hazardous condition exists*. This is a "fail-safe" event, but it has severe economic consequences due to lost production.

- **Cause**: It's typically caused by a "safe" failure of a single component, like a transmitter failing to a high-pressure reading, a wire breaking, or a logic solver card failing.
- **How HIPPS Minimizes It:**
    - **Redundancy in Sensors:** Using 2oo3 voting. If one sensor fails, the other two "out-vote" it, and the process continues. The system is *fault-tolerant* to a single sensor failure.
    - **Redundancy in Logic Solver:** High-integrity logic solvers often use redundant processors (e.g., 1oo2D or 2oo3) that check each other.
    - **Redundancy in Final Elements:** While final elements are often 1oo2 for *safety* (two valves in series), the *control* part (e.g., solenoid valves) might be redundant (e.g., 2oo2) to prevent a single SOV failure from closing the valves.
- This focus on avoiding spurious trips is called enhancing "system availability" or "process availability."

INSTRUNEXUS

What is the relationship between HIPPS and LOPA?

LOPA (Layer of Protection Analysis) is the methodology often used to determine if a HIPPS is required and what SIL it must meet.

- **LOPA Process:**

    - A high-consequence overpressure scenario is identified (e.g., in a HAZOP).
    - The initiating event (e.g., regulator failure) and its frequency are determined.
    - Existing Independent Protection Layers (IPLs) are credited (e.g., alarms with operator action, basic process control).
    - The remaining "risk gap" between the current risk and the company's tolerable risk target is calculated.
- **HIPPS in LOPA:**
    - If a large risk gap remains, a new, high-reliability IPL is needed.
    - A HIPPS is proposed as the SIF (Safety Instrumented Function) to fill this gap.
    - The required Risk Reduction Factor (RRF) to close the gap determines the required SIL. (e.g., if an RRF of 1,500 is needed, a SIL 3 (RRF 1,000-10,000) system is required).
- **In short:** LOPA identifies the problem (the risk gap) and specifies the solution's required strength (the SIL), which the HIPPS must then be designed to meet.

INSTRUNEXUS

Why are HIPPS valves typically "fail-safe" or "de-energize to trip"?

"Fail-safe" (or "de-energize to trip") is a fundamental design principle for safety systems. It means the system will revert to its safest state in the event of a failure of its power or utility supply.

- **HIPPS Application:**
    - The final element valves are almost always "fail-closed" (FC).
    - The actuator (e.g., pneumatic or hydraulic) is designed to *hold the valve open* against a powerful spring.
    - This requires a continuous "energized" signal from the logic solver's output and a continuous supply of power (to the solenoid) and instrument air/hydraulic pressure (to the actuator).
- **Trip Action:**
    - When the logic solver decides to trip, it *de-energizes* its output.
    - This de-energizes the solenoid valve (SOV), which vents the pressure from the actuator.
    - The powerful spring then takes over, forcing the valve to the "safe" (closed) position, thus isolating the high-pressure source.

- **Why it's Safer:** This design automatically handles the most common failures. If a wire is cut, power is lost, or instrument air fails, the system automatically moves to the safe (closed) state. An "energize-to-trip" system would fail dangerously in these scenarios.

What is "diagnostic coverage" (DC) and how does it affect SIL?

Diagnostic Coverage (DC) is a measure of a system's ability to automatically detect its own internal failures.

- **Definition:** It is the ratio of the "dangerous detected" failure rate (λ_DD) to the total "dangerous" failure rate (λ_D_total).
  - DC = λ_DD / (λ_DD + λ_DU)
  - Where λ_DU is the "dangerous undetected" failure rate.
- **How it Affects SIL:**
  - Only *undetected* failures contribute to the PFDavg. The goal of diagnostics is to move failures from the "undetected" (bad) column to the "detected" (good) column.
  - A system with high Diagnostic Coverage (e.g., 90%) will have a much lower PFDavg than a system with low DC (e.g., 0%), even with the same components.
  - **High DC is achieved through:**

    Smart transmitters that check their own electronics.
    Logic solvers with extensive self-checking and redundant processors.
    Partial Stroke Testing (PST), which provides high DC for the mechanical valve.
  - High DC is essential for achieving SIL 3, as it keeps the PFDavg low and can extend test intervals.

INSTRUNEXUS

What does "closing time" mean for a HIPPS valve?

Closing time is a critical performance parameter for the HIPPS final element. It is the total time elapsed from the moment the logic solver initiates a trip signal to the moment the valve is fully closed and has achieved a tight shut-off.

- **Typical Requirement:** This time is often very short, typically in the range of 2 to 5 seconds, but it depends on the specific process.

- **Why it's Critical:**
    - The entire HIPPS system must stop the flow *before* the pressure in the downstream system exceeds its design limit.
    - The process pressure can rise very quickly in some scenarios (e.g., gas blow-by).
    - The allowable closing time is calculated based on the "packing rate" (how fast the downstream pipework pressurizes) and the setpoint of the HIPPS.
- **Components of Closing Time:** It includes the time for:
    - The logic solver to process the signal.
    - The solenoid valve to de-energize and vent.
    - The actuator to move.
    - The valve itself to travel from 100% open to 0% closed.
- This time must be verified during commissioning and re-verified during every full proof test.

Explain "independence" and "separation" in the context of HIPPS.

INSTRUNEXUS

Independence and separation are core principles from IEC 61511, vital for ensuring the integrity of a safety system.

- **Independence:** This means the HIPPS (a SIF) must be independent from the Basic Process Control System (BPCS).
    - The HIPPS sensors, logic solver, and final elements must *not* be used for process control.
    - The *reason* for the demand (e.g., a control valve failing open) cannot be the same reason the protection layer fails (e.g., sharing the same power supply).
    - If the BPCS control loop fails, it must not be able to cause the HIPPS to fail.
- **Separation (Physical & Logical):** This is the *how-to* of achieving independence.
    - Physical: Using separate junction boxes, cable trays, power supplies (e.g., a UPS for the HIPPS), and I/O cards. The HIPPS logic solver must be a separate, certified safety PLC, not the same PLC running process control.
    - Logical: The application logic for the HIPPS must be separate and locked from the BPCS logic.

- **Why it's Critical:** This prevents "common cause failures." If the BPCS and HIPPS shared a power supply, and that power supply failed, you would lose *both* your control and your last line of defense at the same time, leading to a potential disaster.

What is a "Common Cause Failure" (CCF)? Give an example relevant to HIPPS.

A Common Cause Failure (CCF) is the failure of multiple, redundant components or systems due to a single, shared root cause. CCF is the enemy of redundancy and can completely defeat a high-SIL design.

- **Impact:** A 2oo3 sensor system is designed to tolerate one random failure. But a CCF could wipe out all three sensors simultaneously, rendering the PFD calculation invalid and the system useless.
- **Examples Relevant to HIPPS:**
    - **Environmental:** All three pressure transmitters are installed without sunshades in a hot climate. An extreme heatwave causes all three to fail high.
    - **Maintenance Error:** A technician calibrates all three transmitters using the same faulty calibration device, setting them all to read 10% low.
    - **Design Error:** All three transmitters are from the same manufacturing batch, which has a latent defect in a specific microchip.
    - **Process:** The impulse lines (small pipes) leading to all three transmitters become plugged with wax or hydrates from the process fluid. All three sensors will read a stable (but false) pressure.
    - **Power:** All three transmitters are wired to the same power supply, which fails. (This is why separation is critical).
- **Mitigation:** CCF is mitigated by diversity (using different types of sensors), separation(physical/power), and strict maintenance/testing procedures.

BAR·G INSTRUNEXUS

What is the "Proof Test Coverage"?

Proof Test Coverage is the measure of how effective a proof test procedure is at detecting all possible "dangerous undetected" failures in a SIF.

- It is expressed as a percentage. A "perfect" test that finds 100% of all possible hidden faults has a coverage of 100%.
- **Example:** A full "stroke test" of a valve that confirms it moves 0-100% and performs a seat leakage test (e.g., by pressurizing the body) might achieve 95-99% coverage.
- A test that only strokes the valve but doesn't check for leaks might only have 80% coverage, as it could miss a "dangerous" failure (inability to seal).
- **Importance:** The PFDavg calculation assumes a certain proof test coverage. If the actual test procedure used in the field is not as thorough as the one assumed in the design calculation (e.g., the design assumed 95% coverage, but the field test only achieves 70%), then the real-world PFDavg will be higher, and the HIPPS may not meet its required SIL.

What is "diversity" in a HIPPS design?

Diversity is a powerful technique used to protect against Common Cause Failures (CCF). It involves using different components, technologies, or methods to perform the same function.

- **Purpose:** The theory is that a single root cause (like a software bug or a design flaw) is unlikely to affect two completely different types of devices in the same way.
- **Examples in HIPPS:**
  - **Sensor Diversity:** Instead of using three identical pressure transmitters from Manufacturer A, a 2oo3 system might use two from Manufacturer A and one from Manufacturer B (different brand).
  - Or, it might use two pressure transmitters (different technology) and one pressure *switch* (different principle).
  - **Final Element Diversity:** Using a ball valve and a gate valve in series, instead of two identical ball valves.
  - **Logic Solver Diversity:** Using safety PLCs from two different manufacturers for a high-availability, redundant system.
- Diversity is a key strategy, along with separation, to make a redundant system robust against CCF.

INSTRUNEXUS

How is a HIPPS typically bypassed? What are the risks?

A HIPPS bypass is a temporary, controlled measure to take the safety system out of service, usually for maintenance (like a proof test) while the plant continues to run.

- **How it's done:**
  - Bypassing is not just flipping a switch. It is a strict "management of change" (MOC) or "permit-to-work" procedure.
  - A certified safety PLC will have a physical, key-locked "Maintenance Override Switch" (MOS).
  - This switch must be enabled by an authorized person, and it will (or should) trigger a loud alarm in the control room, a flashing light on the panel, and a permanent log in the system's event history.
- **Risks**:
  - The plant is "naked": While on bypass, the last line of defense is gone. The plant is exposed to the overpressure hazard.
  - Human Error: The single biggest risk is forgetting to remove the bypass after the maintenance is complete. Many major industrial accidents have happened because a critical safety system was left on bypass.
- **Risk Mitigation:** Strict procedural controls are required, such as:
  - Time-limited bypasses (e.g., must be re-authorized every 8-hour shift).
  - Requiring "compensating measures," like a dedicated human operator watching the pressure gauge, ready to hit an emergency stop.
  - Audible/visual alarms that cannot be silenced while the bypass is active.

Why are two valves in series (1oo2) often used for the final element?

Using two "fail-closed" valves in series is a redundant architecture (1oo2) designed to enhance the safety of the final element subsystem.

- **Purpose**: It provides fault tolerance against a "dangerous" failure, specifically a "failure to close."
- **Scenario**:
  - A HIPPS is designed to provide a "bubble-tight" or "zero-leakage" shut-off to stop the pressure buildup.
  - If a single valve (1oo1) is used, and it fails to close completely (e.g., it gets stuck 5% open, or the seat is damaged), the overpressure event will not be stopped. The HIPPS will have failed.
  - By using two valves in series (Valve A and Valve B), the system can tolerate one of them failing to close. If Valve A gets stuck, Valve B will still close and isolate the pressure.
- **Note**: This architecture increases safety (lowers PFDavg) but decreases availability. A "safe" failure (one valve closing spurious) will shut down the plant. For HIPPS, safety is always the priority over availability.

What is the "Safety Lifecycle" as defined in IEC 61511?

The Safety Lifecycle is the central concept of IEC 61511. It's a systematic, documented management process that covers all phases of a safety instrumented system, from initial concept to decommissioning.
It ensures that safety is "built-in" and managed at every step, not just added as an afterthought. The main phases are:

- **Analysis Phase:**
  - Hazard and Risk Assessment (HAZOP, LOPA).
  - Allocation of safety functions to protection layers.
  - Writing the Safety Requirements Specification (SRS).
- **Realization (Design & Implementation) Phase:**
  - SIF design and engineering (e.g., designing the HIPPS).
  - SIL verification calculations.
  - Hardware selection, software development.
  - Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT).
  - Installation, commissioning, and final validation.
- **Operation & Maintenance Phase:**

  - Operation and monitoring.
  - Proof testing and inspection at the required intervals.
  - Maintenance and repair.
  - Management of change (MOC).
  - Regular auditing and assessments.
- **Decommissioning Phase:** Safely taking the system out of service.

What is the Safety Requirements Specification (SRS) and why is it the most important document?

The Safety Requirements Specification (SRS) is the foundational document for any SIF, including HIPPS. It is the "bible" that details what the safety system must do, how well it must do it, and under what conditions.
It is arguably the most important document because the entire design, verification, and testing program is based on meeting its requirements. "If it's not in the SRS, it doesn't exist."

INSTRUNEXUS

Key contents of an SRS for a HIPPS:

- **SIF Definition:** A clear description of the overpressure hazard it's protecting against.
- **Inputs & Outputs:** Which pressure transmitters are used, which valves are to be closed.
- **Functional Logic:** The voting (e.g., 2oo3) and the trip setpoint (e.g., trip at 50 barg).
- **Safety Integrity Requirements:**
  - The required SIL (e.g., SIL 3).
  - The required PFDavg (e.g., < 1.0 x 10^{-3}).
- **Performance Requirements:**
  - The required valve closing time (e.g., < 2 seconds).
  - The required leak tightness (e.g., ANSI Class VI).
- **Operational Requirements:**
  - The Proof Test Interval (e.g., 2 years).
  - Requirements for bypassing, alarms, and diagnostics.

What is the difference between "safe" and "dangerous" failures?

In functional safety, failures are categorized based on their impact on the safety function.

- **Safe Failure:**
  - A failure that causes the system to move to its "safe" state, even when no demand is present.
  - Example: A transmitter fails high, a wire breaks, or a power supply fails. This causes the logic solver to "see" a trip and (in a 1oo1 system) close the HIPPS valves.
  - This results in a spurious trip. It's safe, but it stops production and costs money. It affects availability.
- **Dangerous Failure:**
  - A failure that prevents the safety system from working when a real demand occurs.
  - This type of failure is "dormant" or "covert" – you don't know it has happened until it's too late (unless you test for it).
  - Example: A transmitter fails low (or "frozen" at a normal reading), a valve is mechanically stuck open, a logic solver relay is welded shut.
  - This failure affects safety. These are the failures that SIL and PFDavg are designed to manage.
- Failures are further split into Detected (by diagnostics) and Undetected (only found by proof test). The worst kind is a "Dangerous Undetected" (DU) failure.

What is a 1oo2D architecture? How does it differ from 1oo2?

Both are redundant architectures, but they serve different purposes.

- **1oo2 (One-out-of-Two):**
  - Two components (A and B). If either A or B votes to trip, the system trips.
  - **Use:** This is a safety-oriented architecture. It is fault-tolerant to one "dangerous" failure (e.g., if A is stuck, B can still trip).
  - **Example:** Two HIPPS valves in series (1oo2 logic to close). Or two sensors where a trip from either one causes a shutdown.
  - **Downside:** Terrible for availability. A single "safe" failure (a false trip from A) shuts down the plant.

BAR·G INSTRUNEXUS

- **1oo2D (One-out-of-Two with Diagnostics):**
  - Two components (A and B) that are continuously comparing themselves (the "D" for Diagnostics).
  - **Use**: This is an availability-oriented architecture, often used in logic solvers.
  - **Logic**:

    If A and B are "OK," the system runs.
    If A votes to trip, but B is "OK," the system does not trip. Instead, it flags a "discrepancy alarm" for maintenance. It knows A is faulty.
    The system only trips if both A and B vote to trip (making it 2oo2 for tripping) OR if the diagnostics detect a fatal internal error.
  - **Benefit**: It provides high safety (like 2oo2) but also high availability (like 1oo1) by using diagnostics to avoid spurious trips from a single component failure.

What is the role of a Solenoid Valve (SOV) in a HIPPS final element assembly?

INSTRUNEXUS

The Solenoid Valve (SOV) is the "electronic-to-pneumatic" (or hydraulic) interface. It's the fast-acting switch that translates the logic solver's electrical trip signal into the powerful mechanical action of the actuator.

- **Normal Operation (Energized):**
  - The HIPPS logic solver sends a 24VDC (typically) signal, "energizing" the SOV's coil.
  - This holds the SOV in a position that routes instrument air (or hydraulic fluid) *into* the actuator, holding the main HIPPS valve open against its spring.
- **Trip Condition (De-energized):**
  - The logic solver cuts the 24VDC signal.
  - The SOV's internal spring slams it to its "safe" position.
  - This new position blocks the incoming air supply and vents all the air from the actuator to the atmosphere.
  - With the pressure gone, the actuator's powerful spring takes over and slams the main HIPPS valve shut.
- **Redundancy:** Because the SOV is a critical component, it is often made redundant (e.g., 1oo2 or 2oo3 voting) to ensure it vents when required and doesn't vent spuriously.

What is "Prior Use" or "Proven in Use" justification?

This is a provision within IEC 61511 that allows an end-user to select a component for a safety application even if it was not certified by a third party (like TÜV) according to IEC 61508.
To use this justification, the end-user (the plant owner) must take on the burden of proof and provide rigorous, documented evidence that the component is reliable for that specific application. This requires:

- **Extensive Operational History:** A large volume of operating hours (e.g., millions of hours) for the exact component model in a similar service (pressure, temperature, fluid).
- **Robust Failure Data:** Meticulous records of all failures, operating demands, and successful tests for that component population.
- **Data Analysis:** Statistical analysis of this field data to demonstrate that the component's "dangerous failure rate" is low enough to meet the SIL requirements.
- **Management System:** A strict internal system for tracking, analyzing, and managing this data.

It is a difficult and data-intensive path, which is why most companies prefer to buy components that are already "SIL-certified" by the manufacturer.

BAR·G
INSTRUNEXUS

What is a "Functional Safety Assessment" (FSA)?

A Functional Safety Assessment (FSA) is a formal, mandatory audit specified by IEC 61511. It is performed at key stages of the safety lifecycle to ensure that the SIF (e.g., HIPPS) is being designed and managed correctly according to the standard and the SRS.
An FSA is conducted by a competent, independent team (often including at least one person not from the project team).

There are 5 stages of FSA:

- **FSA Stage 1:** After the SRS is complete and before detailed design. (Checks what is to be built).
- **FSA Stage 2:** After the detailed design is complete and before construction. (Checks how it will be built).

- **FSA Stage 3:** After installation, commissioning, and validation, before the hazard is introduced (i.e., before startup). This is the final "gate" to confirm the HIPPS is built as specified and is ready to work.
- **FSA Stage 4:** Periodically during the operation and maintenance phase (e.g., every 3-5 years) to ensure proof tests are being done, MOC is followed, etc.
- **FSA Stage 5:** After any modifications, to ensure safety integrity hasn't been compromised.

What is "SIL Verification" vs. "SIL Validation"?

These two terms are often confused but are distinct, mandatory steps in the lifecycle.

- SIL Verification (The "Paper" Check):
    - **Question:** "Are we building the system right?"
    - **What it is**: A set of calculations and analyses done during the design phase.
    - **Activity:** It involves using reliability data (failure rates) for the chosen sensors, logic solver, and valves, and plugging them into PFDavg formulas (or software).
    - **Goal:** To prove mathematically that the proposed design (e.g., 2oo3 sensors, 1oo2D logic solver, 1oo2 valves, 1-year test interval) will achieve the required PFDavg and thus meet the SIL target (e.g., SIL 3).
- SIL Validation (The "Physical" Check):
    - **Question:** "Did we build the right system?"
    - **What it is:** A physical, hands-on test performed after installation and before startup (as part of Site Acceptance Testing - SAT).
    - **Activity:** It involves testing the entire HIPPS loop "end-to-end." For example, applying a known pressure to the sensors, confirming the logic solver trips at the correct setpoint, and measuring the valves to confirm they close within the specified time.
    - **Goal:** To prove physically that the as-built HIPPS performs exactly as specified in the Safety Requirements Specification (SRS).

INSTRUNEXUS

What is the 'Safe Failure Fraction' (SFF)?

Safe Failure Fraction (SFF) is a concept from IEC 61508. It is a measure of what percentage of *all* failures (safe and dangerous) in a component are "safe" or "dangerous detected."
SFF = (Total Safe Failures + Dangerous Detected Failures) / Total Failures

- It's a measure of the "goodness" or "self-diagnosing" capability of a component. A "smart" transmitter with high internal diagnostics will have a high SFF (e.g., > 90%). A "dumb" component like a mechanical switch will have a low SFF (e.g., < 60%).
- In IEC 61508, the SFF of a subsystem (like the sensors) determines the minimum "Hardware Fault Tolerance" (HFT) required for a given SIL.
- **Example**: To achieve SIL 3 with a component that has a low SFF (60-90%), you must have a Hardware Fault Tolerance of 2 (e.g., a 2oo3 or 1oo3 architecture).
- **Note**: While critical in IEC 61508 (for manufacturers), IEC 61511 (for users) puts more emphasis on the final PFDavg calculation. However, SFF still guides the selection of architectures.

INSTRUNEXUS

What is "Hardware Fault Tolerance" (HFT)?

Hardware Fault Tolerance (HFT) is a measure of a system's redundancy. It is defined as the number of failures the system can tolerate and *still perform its safety function*.
HFT = N - 1 (for 'K out of N' systems where K < N)

- **HFT = 0 (No redundancy):**
  - A 1oo1 architecture (e.g., one sensor, one valve).
  - It has zero fault tolerance. If that one component fails dangerously, the safety function is lost.
- **HFT = 1 (One fault tolerated):**
  - A 1oo2 or 2oo3 architecture.
  - A 1oo2 system can tolerate one component failing "safe" (but will trip).
  - A 2oo3 sensor system can tolerate one sensor failing either "safe" (spurious) or "dangerous" (missed trip) and will still function correctly. This is why it's so popular.
- **HFT = 2 (Two faults tolerated):**

  - A 1oo3 or 2oo4 architecture.
  - A 2oo4 system can tolerate two dangerous failures (in some cases) or two spurious failures.
- IEC 61508 dictates the minimum HFT required for a given SIL, based on the component's SFF.

How do you set the trip point for a HIPPS?

INSTRUNEXUS

The trip setpoint is a critical parameter defined in the SRS. It must be set high enough to avoid spurious trips during normal operation, but low enough to shut down the system *before* the downstream piping/vessel design pressure is exceeded.
The setpoint must account for the entire system's dynamics:

- **Piping/Vessel Design Pressure (MAWP):** This is the hard limit that can *never* be exceeded (e.g., 60 barg).
- **HIPPS Valve Closing Time:** The system takes time to act (e.g., 2 seconds).
- **Process Packing Rate:** How fast the pressure builds up (e.g., 5 bar/second).
- **Sensor/System Inaccuracy:** All instruments have a small error margin.

Calculation (Simplified):

Max Allowable Setpoint = (MAWP) - (Pressure rise during valve closing) - (Safety margin)

- Pressure rise = Packing Rate * Closing Time (e.g., 5 bar/s * 2s = 10 bar)
- Safety Margin = Accounts for instrument error, etc. (e.g., 3 bar)
- Setpoint = 60 barg - 10 bar - 3 bar = 47 barg

This ensures that even if the pressure is rising at its maximum rate, by the time the valves shut at 47 barg, the final "packed" pressure will not exceed 60 barg.

What type of valves are typically used for HIPPS final elements, and why?

The choice of valve is critical for both speed and sealing capability. The most common types are:

- **Trunnion-Mounted Ball Valves:**
  - **Why:** Extremely fast (quarter-turn action), high flow capacity (Cv), and can provide excellent "bubble tight" shut-off (soft or metal-seated). The trunnion support reduces torque, allowing for smaller, faster actuators.
  - **Dominant choice:** This is the most common valve type for HIPPS.
- **Slab Gate Valves (Through-Conduit):**
  - **Why:** Provide a full, unobstructed bore when open, minimizing pressure drop. They offer very tight sealing.
  - **Downside:** Slower than ball valves (multi-turn action, though this can be fast with powerful actuators) and are physically larger.
- **Axial Flow Valves:**
  - **Why:** Very fast-acting, in-line design that is "slam-shut" capable. Often used in high-pressure gas applications.
- **Key Requirements:** Regardless of type, the valve must be "Fire-Safe" (e.g., API 607/6FA) and certified for the required tight shut-off class (e.g., API 598 or FCI 70-2 Class VI).

BAR·G
INSTRUNEXUS

What is a "Safety Manual" for a HIPPS component?

A Safety Manual is a document provided by the manufacturer of an IEC 61508-certified component (like a safety PLC, transmitter, or valve). This document is mandatory for the end-user to correctly integrate the component into a SIF.
It is not a standard instruction manual. It contains all the safety-specific data needed for SIL verification and design, such as:

- **Failure Rate Data:** The "lambda" (λ) values:
  - λ_SU (Safe Undetected)
  - λ_SD (Safe Detected)
  - λ_DU (Dangerous Undetected)
  - λ_DD (Dangerous Detected)
- Safe Failure Fraction (SFF) of the component.
- Hardware Fault Tolerance (HFT) requirements.
- **Constraints on Use:** Any limitations, such as environmental, application, or software versions.

- **Mandatory Proof Test Procedures:** The exact steps the manufacturer requires the end-user to perform during a proof test to validate the component's integrity and maintain the failure-rate claims.

Failing to follow the instructions in the Safety Manual (e.g., using a different proof test) invalidates the certification and the SIL verification.

What are the documentation requirements for a HIPPS?

IEC 61511 places a heavy emphasis on documentation. "If it isn't documented, it didn't happen." All phases of the safety lifecycle must be documented and auditable.

Key documents include:

- **Analysis Phase:**
  - HAZOP and LOPA reports (showing the need for the HIPPS).
  - The Safety Requirements Specification (SRS).
- **Design (Realization) Phase:**
  - SIL Verification Report (the PFDavg calculations).
  - Cause & Effect diagrams, logic diagrams, P&IDs.
  - Hardware and software design specifications.
  - Component Safety Manuals.
  - FAT, SAT, and Validation Test procedures and results.
- **Operation & Maintenance Phase:**
  - Operating procedures (including bypass procedures).
  - Proof Test Procedures.
  - Proof Test Records (signed, dated results of every test).
  - Failure Records: A log of all failures (safe and dangerous), demands, and spurious trips.
  - MOC (Management of Change) Records: Documentation for any change, no matter how small.
  - Functional Safety Assessment (FSA) reports.

BAR·G INSTRUNEXUS

How do you manage "Management of Change" (MOC) for a HIPPS?

Management of Change (MOC) is a formal, documented process for managing any modification to the HIPPS after it has been validated and commissioned. This is one of the most critical O&M procedures.

A "change" can be anything:

- **Obvious Changes:** Replacing a transmitter with a different model, changing the logic solver, changing the valve type.
- **Subtle Changes:** Updating the logic solver's firmware, changing the trip setpoint by 1 bar, extending the proof test interval from 1 to 2 years, changing a setting in a "smart" transmitter.

The MOC process requires:

- **Justification:** Why is the change needed?
- **Impact Analysis (Critical Step):** A formal assessment of how the change will affect the *safety* of the HIPPS. Will it impact the PFDavg? Does the SIL verification need to be re-done?
- **Authorization:** Approval from a competent authority (e.g., the site's technical/safety lead).
- **Implementation**: Making the change.
- **Re-Validation:** Testing the system to prove it still meets the SRS after the change.
- **Documentation:** Updating all affected documents (P&IDs, SRS, verification report) to reflect the "as-built" state.

Failure to follow MOC is a major cause of industrial accidents, as small, undocumented changes slowly erode the safety protection.

What is a "Demand" on a safety system?

A Demand is an event where the process conditions become hazardous (e.g., pressure rises towards the trip point), requiring the safety system to act to return the process to a safe state.

There are two main types of demands:

- **Real Demand (or "Process Demand"):**
  - A genuine, unplanned process upset.
  - Example: A regulator fails, and the pressure genuinely starts to rise, causing the HIPPS to trip.

BAR·G
INSTRUNEXUS

    - All real demands must be logged, investigated (to find the root cause), and documented.
- **Proof Test Demand:**
    - A "fake" demand that is intentionally created by technicians as part of a proof test.
    - Example: Hooking up a hand-pump to a pressure transmitter and raising the pressure to the trip setpoint to watch the system activate.
    - This is the primary way of finding "dangerous undetected" failures.
- The "Probability of Failure on Demand" (PFD) is literally the probability that the HIPPS will fail during one of these "Real Demands."

What is "Competency" in the context of IEC 61511?

Competency is a mandatory requirement from IEC 61511. It states that *all* personnel involved in any safety lifecycle activity must have the necessary knowledge, training, and experience for the specific role they are performing.

INSTRUNEXUS

This is not just a suggestion; it must be formally managed and documented. A company must be able to prove its people are competent.

This applies to everyone:

- Engineers doing the LOPA and SIL verification.
- Designers selecting the components.
- Technicians installing the cable and impulse lines.
- Programmers writing the logic solver code.
- Operators who have to respond to alarms.
- Maintenance staff performing the proof tests.
- Managers overseeing the process and authorizing MOC.

Competency can be demonstrated through:

- Formal training and certification (e.g., CFSE - Certified Functional Safety Expert).
- Verifiable "on-the-job" experience.
- A documented in-house competency management program.

What is the 'Mission Time' of a HIPPS?

Mission Time (or "Design Life") is the overall period for which the HIPPS is designed to operate before it needs major refurbishment or replacement. This is typically set by the end-user and might be 15, 20, or 25 years, often matching the expected life of the plant or facility.

- **Why it matters:**
  - Component failure rates (λ) are not constant forever. The "bathtub curve" shows that after a certain period, components enter a "wear-out" phase where failure rates increase dramatically.
  - The SIL/PFDavg calculations are only valid during the "useful life" of the components, before this wear-out phase begins.
  - The component Safety Manuals may specify a shorter mission time (e.g., "this PLC is designed for a 15-year life").
- This means the company must have a plan to replace or fully refurbish the HIPPS components (especially the logic solver and valves) before their stated mission time expires, otherwise, the SIL rating can no longer be claimed.

INSTRUNEXUS

How should impulse lines for HIPPS sensors be installed?

The impulse lines (the small-bore pipes connecting the process tapping to the pressure transmitters) are a common source of failure. Their correct installation is critical to avoid common cause failures. Best practices include:

- **Independence:** Each transmitter in a 2oo3 arrangement should have its own separate process tapping. They should not share a single tapping, as a plug in that one tapping would defeat all three sensors.
- **Separation:** The impulse lines should be routed separately to avoid physical damage to all of them at once.
- **Slope:**
  - For gas service, the lines should be sloped *down* from the transmitter *to* the process, allowing any condensed liquids to drain back.
  - For liquid service, the lines should be sloped *up* from the transmitter *to* the process (or kept "liquid-full") to allow any trapped gas bubbles to vent back.

- **Isolation:** Each line must have a robust, double-block-and-bleed (DBB) isolation valve arrangement to allow for safe removal and calibration of the transmitter while the process is online.
- **Plugging Prevention:** For "dirty" service (e.g., wax, sand), the tappings should be in a low-velocity area, and heat tracing or periodic flushing may be required.

What is the difference between a "certified" and "non-certified" safety PLC?

This relates to the suitability of the logic solver for a safety function.

- **Non-Certified PLC (A "BPCS" PLC):**
    - This is a standard PLC designed for process control.
    - Design goal: High availability, flexibility, and speed. Safety is not the primary design driver.
    - It has a single processor, simple I/O, and limited self-diagnostics. Its failure modes are unknown and its failure rates are not certified.
    - It is never acceptable to use a BPCS PLC as the logic solver for a HIPPS. This is a fundamental violation of independence (IEC 61511).
- **Certified Safety PLC (A "SIS" PLC):**
    - This is a PLC purpose-built for safety applications and has been certified by an independent body (like TÜV) as compliant with IEC 61508 for use in SIL 2, 3, or 4 applications.
    - Design goal: Extreme reliability, predictability, and failure-safety.
    - Features: It has massive internal redundancy (e.g., 1oo2D or 2oo3 processors), extensive self-diagnostics (high SFF), fault-tolerant I/O, and a read-only, secure operating system.
    - Its failure rates (λ_DU, etc.) are known, certified, and published in its Safety Manual.

BAR·G
INSTRUNEXUS

What is a "Type A" vs. "Type B" component?

This is a classification from IEC 61508 based on the complexity of a component and how well its failure modes are understood.

- **Type A Component:**
  - "Simple" component with well-defined failure modes and behavior.
  - The failure modes of all internal parts are well-understood.
  - There is extensive, reliable field data to back this up.
  - Examples: A simple relay, a fixed resistor, a mechanical pressure switch, a solenoid valve.
- **Type B Component:**
  - "Complex" component, typically containing a microprocessor or complex software.
  - The failure modes are not "fully determined." It's impossible to predict every single way a microprocessor could fail.
  - Examples: A "smart" pressure transmitter, a safety PLC, a digital valve controller (positioner).
- **Why it matters:** The standards (IEC 61508) place stricter requirements on Type B components to achieve a given SIL. For example, to get SIL 3, a Type B subsystem must have a Hardware Fault Tolerance of at least 1 (e.g., 2oo3), whereas a Type A system *might* achieve it with HFT=0 (1oo1) if its failure rates are incredibly low (which is rare).

What is the 'test philosophy' for a 2oo3 sensor setup?

The testing philosophy must be carefully designed to prove the integrity of the voting logic without causing a spurious trip. This is typically done "online" (while the process is running).

The procedure is:

- **Bypass one channel:** The technician puts only one sensor (e.g., Transmitter A) into a "test" or "bypass" mode in the logic solver. The HIPPS is now temporarily operating in a 2oo2logic on Transmitters B and C.
- **Isolate and Test:** The technician closes the process isolation valve for Transmitter A and applies a test pressure (from a hand pump) to it.

BAR·G
INSTRUNEXUS

- **Verify Trip:** The technician confirms that the logic solver "sees" the trip signal from Transmitter A (even though it's bypassed and won't trip the plant). This confirms the transmitter and its wiring are good.
- **Restore and Un-bypass:** The technician restores Transmitter A to service and removes the bypass. The system is back in 2oo3 mode.
- **Repeat:** The process is repeated for Transmitter B (with A and C in 2oo2 logic) and then for Transmitter C (with A and B in 2oo2 logic).

This one-at-a-time method allows the full testing of each sensor channel without ever shutting down the process, thus maintaining high availability.

What is the 'Mean Time To Repair' (MTTR) and how does it affect HIPPS?

INSTRUNEXUS

MTTR (Mean Time To Repair) is the average time it takes to detect a failure, diagnose the problem, get the spare part, repair the component, and restore the system to full function.

- **Impact on 'Safe' Failures (Availability):**
  - If a HIPPS component fails "safe" in a 1oo2 or 2oo3 system (e.g., one sensor fails high), it creates an alarm but doesn't shut down the plant.
  - The plant is now running in a "degraded" state (e.g., 2oo2). It has lost its fault tolerance. If a second failure occurs, it will cause a spurious trip.
  - The MTTR is the "window of exposure" to this spurious trip. A low MTTR (e.g., 4 hours) is critical for maintaining high plant availability. This is why having spare parts on-site is essential.
- **Impact on 'Dangerous' Failures (Safety):**
  - For detected dangerous failures (found by diagnostics), the MTTR is the time the plant is exposed to that "known" fault.
  - A long MTTR for a "dangerous detected" fault could require the plant to be shut down.
  - In PFDavg calculations, MTTR is a key factor for redundant systems.

Can a PSV be installed *downstream* of a HIPPS?

Yes, and this is a very common design. The downstream system (the LP system) will almost always have its own conventional Pressure Safety Valve (PSV) as a final, final line of defense.
The safety layers are "stacked" as follows:

- **Basic Process Control System (BPCS):** A control valve tries to regulate the pressure. (e.g., set at 30 bar).
- **BPCS Alarm**: A high-pressure alarm for the operator (e.g., at 40 bar).
- **HIPPS (The SIF):** This is the primary overpressure protection. (e.g., trips at 47 bar).
- **Downstream PSV:** This is the final, passive safety device. It is set higher than the HIPPS but at or below the vessel's MAWP. (e.g., set to open at 60 bar).

Why have both?

- The HIPPS is designed to prevent the PSV from ever lifting. The goal of HIPPS is containment.
- The PSV is there to protect against scenarios that the HIPPS doesn't protect against (e.g., a fire/external heat source causing thermal expansion) or in the extremely unlikely event of a HIPPS failure.
- Because the HIPPS handles the main overpressure scenario (e.g., regulator failure), the downstream PSV can often be much smaller, sized only for "secondary" cases like thermal expansion. This saves significant cost on flare systems.

BAR·G
INSTRUNEXUS

What is a "security assessment" in IEC 61511?

This is a relatively new but critical requirement, added in the 2016 edition of IEC 61511. It recognizes that safety systems (which are now networked digital devices) are vulnerable to cybersecurity threats. A Security Risk Assessment (or Cybersecurity Assessment) must be performed on the HIPPS to protect against malicious or unauthorized access.

The assessment must identify:

- **Vulnerabilities**: e.g., an open network port on the PLC, a default password that was never changed, a laptop with the programming software that could be stolen.
- **Threats**: e.g., a disgruntled employee, a hacker, malware.

- **Consequences**: e.g., A hacker remotely bypassing the HIPPS, or changing the trip setpoint, or forcing the valves closed to stop production.

Mitigations: Based on the assessment, mitigations must be put in place, such as:

- Physical security (locked cabinets/rooms).
- Network firewalls and data diodes.
- Strict password policies and user access controls.
- Disabling unused ports.
- Antivirus software and patch management (done in a very controlled way).

What is the 'Reset' logic for a HIPPS?

A HIPPS trip must always be a "latching" function. This means that even if the high pressure goes away, the system must not automatically reset itself. It must remain in the safe (tripped) state until a human operator intervenes.

The reset logic is a critical part of the design:

- **Manual Reset:** The system must be reset by a deliberate, manual action from a trained operator (e.g., pressing a "Reset" button in the control room).
- **Reset Inhibit:** The logic must be programmed to prevent a reset until the process condition is back to a safe state. (e.g., the reset button will not work until the pressure transmitters read below a "reset permissive" setpoint).
- **Investigation First:** This manual latching function forces the operator to investigate why the HIPPS tripped in the first place before restarting the process. Blindly resetting a safety system can lead to a second, more dangerous event.
- The reset button itself must be physically separate from the BPCS operator screen, often requiring a dedicated, hard-wired pushbutton.

INSTRUNEXUS

What is a "Discrepancy Alarm"?

A Discrepancy Alarm is a key diagnostic feature of a redundant system, like the 2oo3 sensors in a HIPPS.

- **How it works:** The logic solver is continuously comparing the live readings from all three transmitters.

- If one transmitter's reading (e.g., Tx-A reads 35 bar) "deviates" from the other two (e.g., Tx-B and Tx-C read 30 bar) by more than a pre-set amount (e.g., 2 bar), the logic solver generates a "Discrepancy Alarm" or "Voting Alarm."
- **Action:** This alarm is *no a trip. It is an "Urgent Maintenance" alarm sent to the operators and technicians.
- **Meaning:** It tells the staff, "The HIPPS is still working (in 2oo2 mode), but one of its sensors is faulty. You must repair it."
- This is the mechanism that allows the system to be fault-tolerant and allows for online maintenance, achieving both safety and high availability. It is the "call to action" to start the MTTR clock.

What is the difference between HIPPS and HIPS?

This is largely a matter of semantics, but there is a subtle, generally accepted difference:

- **HIPS (High Integrity Protection System):**
  - This is often used as a more general term.
  - It can refer to any high-integrity (SIL 2 or 3) system designed to protect against any hazard, not just pressure.
  - Example: A HIPS could be a SIL 3 system designed to prevent a furnace explosion by shutting off fuel on a "low-flow" or "flame-out" condition.
- **HIPPS (High Integrity *ressure Protection System):**
  - This is a specific type of HIPS.
  - Its one and only purpose is to protect against over-pressurization.
- **In short:** All HIPPS are HIPS, but not all HIPS are HIPPS. That said, in many companies and contexts, the terms are used interchangeably, with "HIPS" being more common. It's always good to clarify the specific hazard being protected against.

BAR·G
INSTRUNEXUS

What is "Systematic Capability" (SC)?

Systematic Capability (SC), formerly known as "systematic integrity," is a concept from IEC 61508 that addresses a component's or system's robustness against systematic failures. It is just as important as the PFDavg (which only handles random failures).

- **Systematic Failures:** These are "bugs" or "flaws" built into the system during its creation. They are not random.
    - A software bug in the PLC's operating system.
    - A specification error in the SRS (e.g., writing the wrong setpoint).
    - A mistake in the PFDavg calculation.
    - A poorly written proof test procedure that misses a key step.
- **SC Rating:** A certified component is given an SC rating (e.g., SC 2, SC 3) based on the rigor of the manufacturer's design, development, and quality control process. A component with an "SC 3" rating was built under extremely strict quality management and is trusted to be used in a SIL 3 function.
- **Rule:** You cannot build a SIL 3 SIF (like a HIPPS) using a component that only has a Systematic Capability of SC 2, even if the PFDavg calculations work out. The entire function is "limited" by the lowest SC rating of any of its components.

If a HIPPS valve passes a Partial Stroke Test (PST), is it guaranteed to work?

INSTRUNEXUS

No, absolutely not. This is a critical limitation to understand.
A successful PST provides a high degree of confidence, but it is not a guarantee.

What a PST does find (its benefits):

- It proves the logic solver output works.
- It proves the SOV works.
- It proves the actuator has power/air and is mechanically free.
- It proves the valve is not "stuck" in the fully open position (e.g., due to corrosion, stiction).

What a PST cannot find (its limitations):

- **Sealing Capability:** It cannot prove the valve will provide a "tight shut-off." The valve seat could be damaged, eroded, or have debris on it, but the PST would not know.

- **Full Stroke Capability:** It cannot prove the valve can travel the last 10-20% of its stroke. The valve could be obstructed by debris only in the last part of its travel.
- **Closing Time:** While it can estimate the time, it doesn't always prove the full, dynamic closing time under process flow.

This is precisely why PST is only a supplement and can never replace the full proof test, which must stroke the valve 100% and (ideally) perform a leak test to verify sealing integrity.

Prepared By,

www.instrunexus.com

Raja Mohanam

Instrumentation

Control & Safety Systems

EPC & FEED

Mentor and Trainer

Focused on interview prep, career growth & simplifying complex concepts in Oil & Gas instrumentation.

admin@instrunexus.com