OFFSHORE PLATFORM SAFETY SHUT-DOWN SYSTEM EFFECTIVENESS

L. Benedicto
Mobil Research & Development Corporation
Dallas,Texas 75381

Steven T. Maher, Shelagh J. Morandini, Barry D. Sloane, and H.L. Phillippi
Westinghouse
Risk Management and Operations Improvement
P.O. Box 355
Pittsburgh, Pennsylvania 15230

ABSTRACT

Quantitative risk assessment techniques are increasingly being applied to facilities that involve (or are perceived to involve) hazardous processes. A fault tree analysis was performed for three standardized design classes of offshore platforms to predict the frequency of the failure of the platform safety shut-down system (PSSDS) to mitigate such hazards as overpressure, fires, explosions, releases of flammable or toxic materials, vessel and compressor knockout drum overfill, and gas blowby. The analysis evaluated the logic processing units (LPU) (both electronic and pneumatic), end-devices, and sensors, and calculated PSSDS unavailability in response to a challenge (covert fault). Platform risk was categorized through the assignment of specific consequence categories to each hazard type. A calculation of platform nuisance shut-down (overt fault) frequency as also performed.

The fault tree models developed for the platforms provided the basis for sensitivity studies which examined a number of design and operations modifications that included:

- redundant/diverse sensors
- redundant/diverse end-devices
- pneumatic and programmable electronic system (PES) architectures
- test & preventive maintenance frequencies
- intrinsically-safe vs. explosion-proof devices
- digital switches vs. analog transmitters
- feedback verification
- multiple flowline - single ESD valve

This provided a firm basis to the designer and to management for the definition of optimized design and operations schemes for the next generation of offshore platforms.

RISK AND HAZARDS MANAGEMENT IN THE 90'S

Industrial accidents have occurred that have been an ominous reminder of the potential for injury and environmental damage. Industrial safety and protecting our environment are important and must be a priority for everyone - especially those individuals within industry charged with responsibilities of loss prevention and hazard management. This has provided a driving force for safety and environmental protection that has prompted many companies to take proactive steps to identify potential hazards and implement modifications to design or operations to help control potential risks.

In addition, government legislation is rapidly evolving and is providing an impetus to facility owners to implement risk management plans that evaluate the safety

aspects of proposed designs or validate the safety of operating plants. Appropriately implemented, risk and hazards management provides distinct benefits to the facility owner by allowing for both cost-effective and safety-conscious decisions pertaining to design and operations.

These developments have prompted industry to scrutinize their operations for risks to the public, employees, environment, and possible loss of capital investment and production. High capital costs of facilities and lower profit margins mandate high plant utilization factors and the avoidance of the widespread impact of accidents. Computerized, state-of-the-art quantitative risk and hazards management technologies are seeing increased use by industry to ensure financial viability of its operations. The sensible application of these techniques provides many tangible benefits for both society and industry.

Over the next few years, Mobil will embark on the development of the detailed design of the next generation offshore Platform Safety Shut-down Systems (PSSDS). Stemming from general industry concerns regarding safety and environmental protection, this safety effectiveness project is part of parallel efforts to optimize the design and operations of the PSSDS used to protect offshore platforms.

This project evaluated the base design and also many possible design modifications and architectures for each platform type. The three types of standardized offshore platform designs that were evaluated are categorized into design classes based on the number of shut-down loops in the PSSDS:

- Type I - 50 inputs/outputs - Remote Wellhead Platform
- Type II - 500 inputs/outputs - Production Platform
- Type III - 1500 inputs/outputs - Extensive Production Platform

GENERAL APPROACH FOR SAFETY EFFECTIVENESS

Given that a company has made the commitment to take a proactive stance to achieve a greater degree of safety and improve nuisance shut-down frequency for a new design, an effective approach must be chosen. The approach must balance the likelihood of an undesirable event (safety hazard or nuisance shut-down) with the consequences of the event should it occur (injury, environmental damage, capital losses). Safety effectiveness was defined for this project as the ability of the PSSDS to provide sufficient reliability to protect an offshore platform without a significant increase in the frequency of nuisance shut-downs. The approach chosen for assessing the safety effectiveness of an offshore platform had to be efficient, make good use of manpower resources, and provide a firm basis to the designer and to management for the definition of optimum design and operations schemes.

A quantitative risk assessment (QRA) based approach was chosen. This project performed a quantitative analysis of the availability of each platform safety shut-down system (PSSDS) loop in response to a challenge, and assessed the advantages of a number of alternative configurations, in order to identify ways to improve PSSDS availability in a cost-effective manner.

TOOLS USED FOR QUANTITATIVE RISK ASSESSMENT (QRA)

Hazards and availability problems that have been identified through any number of ways [e.g. history of known problems in a system, Hazard and Operability Studies (HAZOPS), Failure Modes, Effects, and Criticality Analysis (FMECA)] can be systematically analyzed, evaluated and documented using fault tree analysis (FTA), event tree analysis (ETA), and consequence analysis. Consequence analysis examines the impact of the identified problems on equipment, personnel, the environment, and the public.

This project utilized fault trees that modeled failures leading to PSSDS shut-down loop unavailability. Fault tree analysis systematically identifies, models, analyzes, and documents potential safety or reliability problems. Fault trees are logical structures which describe the causal relationship between the basic hardware, human, and environmental events resulting in system failure. The failures may include random component failures, common cause failures, human errors, and test and maintenance unavailabilities. Boolean algebra techniques are used to quantify the probability of the occurrence of the top level undesired event, using the contributing probability of lower level events.

For this project, Failure Modes, Effects, and Criticality Analysis (FMECA) was used to identify specific equipment failures within the shut-down loops that result in nuisance shut-downs of the PSSDS. Failure probabilities for each of the PSSDS equipment failures were identified in the FMECA table, frequency contribution calculated, and totaled to calculate the frequency of nuisance shut-downs. All the components/failure modes were grouped by nuisance shut-down category to identify the "criticality" of the failure.

Together, these analytical techniques provide meaningful decision-making tools for risk management and loss prevention to assist in making educated decisions to optimize a system with respect to safety and cost. By weighing the probability of a given undesired event versus its safety and financial consequences, one can identify dominant contributors and recommend effective methods to reduce risk or improve reliability to acceptable levels.

Models were constructed using interactive computer methods for fault tree development and solution to systematize and expedite the PSSDS analysis substantially.

These "living" computer models of the physical system can be readily changed to reflect the sensitivity of risk or reliability to design or operations changes.

Together these tools were used to provide a quantitative basis for calculating PSSDS availability and also a basis for the determination of the safety effectiveness of protection systems.

APPROACH FOR THE ASSESSMENT OF SAFETY AND NUISANCE SHUT-DOWN FREQUENCY

A detailed fault tree analysis was performed for the three standardized design classes of offshore platforms to evaluate the frequency of the failure of the platform safety shut-down system (PSSDS) to mitigate hazards. The analysis evaluated the logic processing units (LPU) (both electronic and pneumatic), end-devices, and sensors and calculated PSSDS unavailability in response to a challenge.

The determination of PSSDS effectiveness balanced the calculated PSSDS availability with the significance of the consequences of the hazard should the PSSDS fail. The failure of each specific PSSDS shut-down loop was categorized by consequence. This categorization facilitated a potential later use of the results of this study to directly calculate risk factoring in both the PSSDS challenging frequency and the consequences of the failure of the PSSDS shut-down loop combinations.

PSSDS shut-down loop availability is the primary basis for decision-making for this study. In lieu of a specific risk calculation, a simplified approach to generate target PSSDS unavailability values from identified threshold hazard rates was used for comparison with the calculated PSSDS shut-down loop unavailabilities. The generation of target PSSDS unavailability values relied on some assumptions regarding acceptability. For this study, a Type III platform was used as the basis for the choice of the platform hazard rate for the most severe hazards present at the platform. Since the consequences associated with the most severe hazards have a similar degree of unacceptability from platform to platform, this total platform hazard rate was assumed to apply to other platform types as well. From the hazard rate applied to the most limiting categories, target PSSDS unavailabilities for other consequence categories were calculated from the relative importance of the consequences.

Calculated shut-down loop unavailability target values were calculated for the average shut-down loop (i.e., assuming all shut-down loops exposed to an identical challenging frequency) and for a more limiting fraction of shut-down loops that were assumed to be challenged at a much higher frequency. The determination of necessary design or operations modifications was based on a comparison of the results of the detailed PSSDS unavailability quantification to both target values.

RESULTS & RECOMMENDATIONS

The purpose of this section is to summarize recommendations, observations, and insights extracted from the detailed analyses performed for the project.

In general, the guidance provided in API RP 14C (API Recommended Practice 14C, "Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms," Fourth Edition, September 1, 1986.) for PSSDS design had been followed as part of the design process. Therefore, as a result of this project, there was no mandate for a comprehensive redesign of the PSSDS or special actions necessary to secure the safety of platform personnel. In general, the pedigree of the PSSDS design is consistent with or superior to engineering practices employed throughout the chemical and petroleum industries, and the results of this study indicated no undue or atypical safety hazards to the public, environment, or platform personnel as a result of PSSDS unavailability. Some potential weaknesses and marginal features were identified and changes to design or operations that could provide a cost-effective enhancement of safety systems are being considered.

The absence of recommendations for substantial changes to PSSDS design should not be surprising. Although the analysis performed for this effectiveness study, involving the quantitative balancing of the consequences and the likelihood of an event, has not generally been performed in industry for all platforms, many of these aspects are considered by engineers during the design process. Typically, design engineers (often implicitly) qualitatively balance the likelihood of an event with the resultant consequences of a potential accident to gauge redundancy requirements, equipment reliability requirements, etc. This Effectiveness Study quantitatively and independently evaluated the PSSDS and identified the benefit of the following design practices, which have come into use during the evolution of PSSDS designs and that contribute to the inherent safety of current platform designs:

- Use of Programmable Electronic Systems (PES)
- Use of Redundancy in PES/Logic Processing Unit (LPU)
- "Fail-Safe" Designs and Passive Safety Devices (e.g., PSV)
- Intrinsically Safe (I-S) Designs
- High Pedigree/Reliability Equipment
- Avoidance of Common Equipment and the Potential for Common Mode Failure
- PES/LPU Self-Testing
- Regimented Test/Preventive Maintenance (PM) Programs
- Selective Application of Redundancy & Diversity

General Design & Operations Features, Results, and Recommendations

There are many common features that permeate the various platform types, and the specific analyses performed for the platforms identified many results that applied to all three platform types. The following are some of the more significant results:

Importance of Equipment Outside the LPU Boundary to Total PSSDS Effectiveness - For all the shut-down loops examined, the failure of the end-devices or pilot valves associated with the end-devices, the failure of the actuation signal (e.g., sensors), or the failure of the operator to properly restore the system following test or maintenance dominated shut-down loop unavailability (see Figure 1).

Use of Same End-Device for Multiple Shut-down Loops - The designer should be especially wary of implementing primary redundant or secondary protective features utilizing the same end-devices as the primary protection shut-down loop. The addition of a redundant sensor may not provide the improvement in shut-down loop unavailability that might be anticipated from a superficial examination of the design. This diversity dilemma is a very common conceptual problem for designers which transcends all industries and applies to all platforms.

For cases where primary redundant or secondary protection were provided according to the guidelines of API RP 14C and use unrelated hardware, loop availability was greatly increased.

Sensitivity of LPU Architecture on PSSDS Effectiveness - If a PES is used, unavailabilities for shut-down loops are usually insensitive to the type of PES in place because the PES is not a dominant contributor to shut-down loop unavailability (see Figure 2) except in cases of very long self-test intervals for low redundancy PES configurations.

For pneumatic shut-down loops associated with a Type I platform, LPU availability is balanced with respect to PSSDS shut-down loop availability (i.e., the contribution to shut-down loop unavailability from the end-devices and control elements is of a similar magnitude). In general, the evolution of the PES for PSSDS LPU use and the unavailability associated with these PES designs has advanced well ahead of unavailabilities associated with end-devices, pilot valves, and sensors that typically dominate shut-down loop unavailability. The attention of the protection system design engineer has typically focused on the very reliable LPU and not on the less reliable end-devices, pilot valves, and sensors, sometimes resulting in an unbalanced overall PSSDS design. Additional attention should be focused on the larger contributors to PSSDS unavailability.

Multiple Flowline, Single ESD Valve - For some shut-down loops whose unavailabilities were dominated by the potential failure to close the well and flowline safety valves, significant improvements in shut-down loop unavailability through the addition of a multiple flowline, single ESD valve were identified.

Component Test/Preventive Maintenance Intervals - The impact of a spectrum of test/PM intervals on shut-down loop unavailability was explicitly analyzed. Optimum intervals for component testing typically fell into the 1-month range (see Figure 3). This verified the appropriateness of test/PM intervals typically used for the more complex, manned platforms (4 weeks) and identified the importance of applying these testing intervals to less complex, unmanned/unattended platforms. It should be noted that this optimum test/PM interval is consistent with practices recommended in OCS Order No. 5 (OCS Order No. 5, "United States Department of the Interior Geological Survey Conservation Division, Gulf of Mexico Region, Production Safety Systems," January 1, 1980).

For cases where less frequent testing/PM is performed, adjustments in test/PM interval may not necessarily involve increased costs (Maher, S.T. and R.K. Rodibaugh, "Relief Valve Testing Interval Optimization Program for the Cost-effective Control of Major Hazards," Second Symposium on Preventing Major Chemical Accidents, Oslo, May 1988). Using the identified dominant equipment failure contributors, test/PM frequency for dominant contributors can be increased (more costly), but test/PM for lesser contributors can be decreased (savings).

Maintenance Practices - Much of the equipment used in the platform is of vital importance to safety and operability. A high priority on maintaining the operability of critical equipment through training and use of high quality personnel and procedures should be continued.

The prioritization and dominant contributors identified for each of the platform analyses can be used to develop a critical equipment list, if not already in use, for operations and maintenance personnel. This could be used to identify equipment for which the causes of failures should be identified and addressed, along with the failures themselves, so that related or repeated failures can be avoided. This action would also help to draw attention to critical equipment to ensure proper prioritization by maintenance personnel. Thus, the results of this project are useful for a reliability centered maintenance program.

Test/Preventive Maintenance Activities - Test/PM activities should include a full functional verification of the ability of the component to perform in response to a PSSDS challenge.

Feedback Verification - The unavailability of some shut-down loops is dominated by the failure of the primary protection feature. The addition of feedback verification to

activate a secondary or redundant primary protection feature (in the event the primary failed) would be expected to yield significant improvements in PSSDS unavailability for feedback verification methods that employ a sensor which provides a direct indication of functionality (i.e., limit switch or flow switch).

Intrinsically-Safe (I-S) PSSDS - For a representative shut-down loop, the unavailability of the explosion-proof design is not as good as the intrinsically-safe design. Continued use of I-S architectures in all future PSSDS designs should be followed.

The additional components associated with the I-S shut-down loop configuration were not significant contributors to unavailability. The higher failure rates of the explosion-proof components (due to environmental factors) resulted in a higher loop unavailability. The I-S loop has a better unavailability due to the advantages offered by hermetically sealed components and operation at lower currents than the explosion-proof devices.

I-S configurations would be expected to have not only lower shut-down loop unavailabilities, but also decreased nuisance shut-down frequencies, reduced maintenance requirements (cost and safety impact), and direct improvement in the intrinsic safety of the maintenance activity.

Importance of Downstream Sensors - For some shut-down loops, downstream sensors are critical secondary protection features. Platform personnel should recognize that the removal of sensors may impact not only the immediate component, but could also disable secondary protection features for upstream equipment. If removal or bypass is frequently performed, another means of secondary protection may be required.

Line Integrity Monitoring (LIM) - The fault tree models created for this study explicitly model ground/short failures which result in fail-to-danger conditions. The results indicate that these failures are very insignificant contributors to shut-down loop unavailability. Therefore, LIM is not necessary for maintaining the degree of shut-down loop reliability calculated in this study. Those results apply to the typical fail-safe shut-down loops (de-energized when failed) and electric floating power systems.

"Watchdog Circuitry" - The platform operator must test safety system operation to maintain safety system reliability; however, this testing must be accomplished without shutting-down the platform. Therefore, bypassing safety systems on a periodic basis is necessary. One of the potential failures which were modeled in this study was a failure of the operator to restore the PES to an operable state following test or preventive maintenance. Given the level of sophistication capable in today's PES, automatic PES features (e.g., "watchdog circuitry") could minimize this potential. The following additional capabilities could be desirable for a PES:

- Alarm and flashing light if input or output signal is bypassed
- Periodic re-alarm for shut-down loops which are bypassed for a significant period of time after being initially acknowledged by the operator
- Automatic implementation of the actions associated with that shut-down loop (with pre-alarm prior to timeout) for critical shut-down loops if bypassed for a significant period of time.

These circuits should be designed such that it is extremely difficult for the operator to defeat or bypass the watchdog circuits. As for so many things associated with the operation of any industrial facility, proper management and administrative controls are a very important factor in safe plant operations.

Specific Design & Operations Recommendations for the Platform Designs

The primary purpose of this project was to develop and use decision-making tools for the investigation of potential design or operations modifications which include:

- Addition or Removal of Redundancy
- Modification of Test/Preventive Maintenance Schedules
- Component Replacement with One of Improved Reliability / Pedigree
- System Simplification - reducing the number of components involved in actuating a safety function could improve system reliability by reducing the number of potential failures which could disable the PSSDS and also simultaneously reduce nuisance shut-down frequency
- Addition or Removal of Diversity

Many of the above types of potential improvements were explicitly modeled in the form of sensitivity studies for the platform designs. One example is the modeling of various pneumatic logic/PES combinations which was one of the major objectives of the study.

For all platforms, there were many cases where the addition of redundancy or the improvement in component reliability of specific less-expensive devices that dominated PSSDS unavailability often provided cost-effective improvements in unavailability and are under consideration.

For all platforms, adherence to high quality standards for vendor specifications and inexpensive improvements to the reliabilities of the following types of more expensive components and/or their associated pilot valves would improve PSSDS reliability and are being considered:

- Subsurface Safety Valves (Downhole Valves)
- Surface Safety Valves (Master Valves)
- Flowline Flow Safety Valve

TYPE I

Given the potential consequences associated with the failure of the Fire/ESD shut-down loop, the addition of both the multiple flowline/single ESD valve and a 1oo1 PES are being considered for this shut-down loop.

TYPE II

The following are some of the items being considered based on a review of the dominant contributors to failure for each shut-down loop:

- Implementation of non-mechanically interlocked 100% capacity PSVs with staggered setpoints wherever two - 50% capacity valves or a single 100% capacity valve is now in use (applies to Type II and Type III). For cases where the operating pressure is very close to vessel design pressure, it may be necessary to utilize dual 100% capacity PSVs which have the same setpoints and are mechanically interlocked.
- Reconfiguration of the general PSV/FSV arrangement on each vessel's passive relief system taking into account PSSDS unavailability and the potential for maintenance personnel injury during maintenance. Reconfigurations could include removal of other devices in the PSV path or adding manual block valves in the PSV path to provide maintenance flexibility and more positive isolation of the Flare System (applies to Type II and Type III).
- For a pump on a process vessel liquid outlet line, the designer should verify the existence of a primary protection feature of the pump shutting down on LSL in the supply vessel. In some cases, the designer may wish to install a secondary or primary redundant protective feature (applies to Type II and Type III).
- For a LSH shut-down loop on process vessels upstream of a compressor, a redundant primary or secondary protection feature if none exists may be required (applies to Type II and Type III).
- For a VSH shut-down loop, the addition of a redundant or diverse isolation device actuated from redundant or diverse sensors.
- For the "I" Shut-down Loop (Type II) and fire and gas release shut-down loops (Type III):
  - the addition of redundant blowdown valves or pressure control valves on critical process vessels
  - maintaining the use of high reliability end-devices and management controls
  - minor modifications to the "I" Shut-down Loop logic

TYPE III

Although the Type II and Type III platforms differ in size and complexity there is a significant similarity in the configuration and effect on platform unavailability for each shut-down loop on a case-by-case basis.

The following are some of the items being considered based on a review of the dominant contributors to failure for each shut-down loop:

- Redundant or diverse emergency shut-down valves (and pilot valves) in series with existing ones for critical shut-down loop actions.
- An additional 100% capacity PSV on the Recompressor.
- For the fire and gas release shut-down loops:
- Addition of a second valve in series with an existing shut-down valve for critical fire loops.
- Addition of a multiple flowline, single ESD valve. This feature, applied to well flowlines, would provide an additional margin to safety and can be fairly cost-effective in terms of risk improvement. The trend in industry has been toward increasingly larger platforms which accommodate greater numbers of wells. The more wells feeding a platform, the more likely a system is to fail to shut-in in the event of a fire or large gas release and also the larger the consequences. This could imply that designers should consider smaller platform designs accommodating fewer wells; however, economic driving forces are mandating larger, more complex platforms. Manifolding of wells at various points in the system and the addition of multiple flowline, single ESD valves may provide a more cost-effective alternative and the necessary isolation abilities.
- 2oo3 gas detection architecture as the standard design configuration - The analysis of the gas detection shut-down loop indicates that a 2oo3 detector architecture improves the unavailability associated with gas detection and results in a lower nuisance shut-down frequency contribution from the gas detectors.

CONCLUSIONS

Since the guidance provided by API RP 14C for PSSDS design was followed during the initial design process, there was no mandate for a comprehensive redesign of

the PSSDS or special actions necessary to secure the safety of platform personnel. In general, the pedigree of the PSSDS design is consistent with or superior to engineering practices employed throughout the chemical and petroleum industries, and the results of this study indicated no undue or atypical safety hazards to the public, environment, or platform personnel as a result of PSSDS unavailability. Some potential weaknesses and marginal features were identified and changes to design or operations which could provide a cost-effective enhancement of safety systems are being considered.

Although all possible configurations could not possibly have been modeled, the detailed PSSDS models evaluated a significant number of design and operations alternatives. The models and documentation provide tools to the designer and operations manager to address questions or concerns not explicitly evaluated for this study.

The approach used in this study (i.e., detailed modeling of the PSSDS and categorization of shut-down loops by consequence category) provided an initial vehicle for making decisions on the optimal configuration from a design and operations perspective. The primary decision-making basis for the project recommendations is PSSDS shut-down loop unavailability in response to a challenge of the PSSDS. Although this provided a good basis for making decisions as part of the design process, a more complete risk perspective can be provided by explicitly modeling two additional parameters:

- frequency of challenges (PSSDS demand rate) to the PSSDS, and
- significance of the consequences should the protective measures fail

The approach chosen and the structure and quality of this analysis provides a vehicle for an extension into risk-based decision-making. Augmenting the study by determining the magnitude of the consequences and PSSDS challenging frequency may be used to clarify the need and priority for design and operations modifications or fundamental changes to PSSDS architecture on a case-by-case basis.

Possible Activities to Augment or Enhance the PSSDS Effectiveness Study

This project addressed the most important characteristics of the PSSDS, identified potential weaknesses, modifications to address those weaknesses, and provided a tool for the design engineer to optimize PSSDS design. However, the following activities could provide additional benefits using the software models developed for the project.

- Performance of a well-focused, specific PSSDS analysis for new platforms in the design phase or for major changes to existing platforms prior to design finalization. These analyses could be done on a priority basis for more complex platform designs and updated during the life of the platform using the "living" software models created for the project whenever safety significant changes to design or operations are made.
- Initiation of a program to collect, analyze, and then integrate company-specific equipment failure data with industry data. This higher pedigree data base can be used with the models created for this project to create a more useful "living" model which can provide an improved basis for risk-based decision-making throughout the life of the facility.
- Reliability Centered Maintenance (RCM) balances system reliability and safety concerns to optimize maintenance intervals and practices. RCM also monitors the effectiveness of maintenance practices and feeds that information back into the determination of optimal maintenance intervals and practices. A RCM program could be readily integrated with the models created for this project.

FIGURE 1

UNAVAILABILITY CONTRIBUTION OF SAMPLE PSL LOOP FOR TYPE II PLATFORM

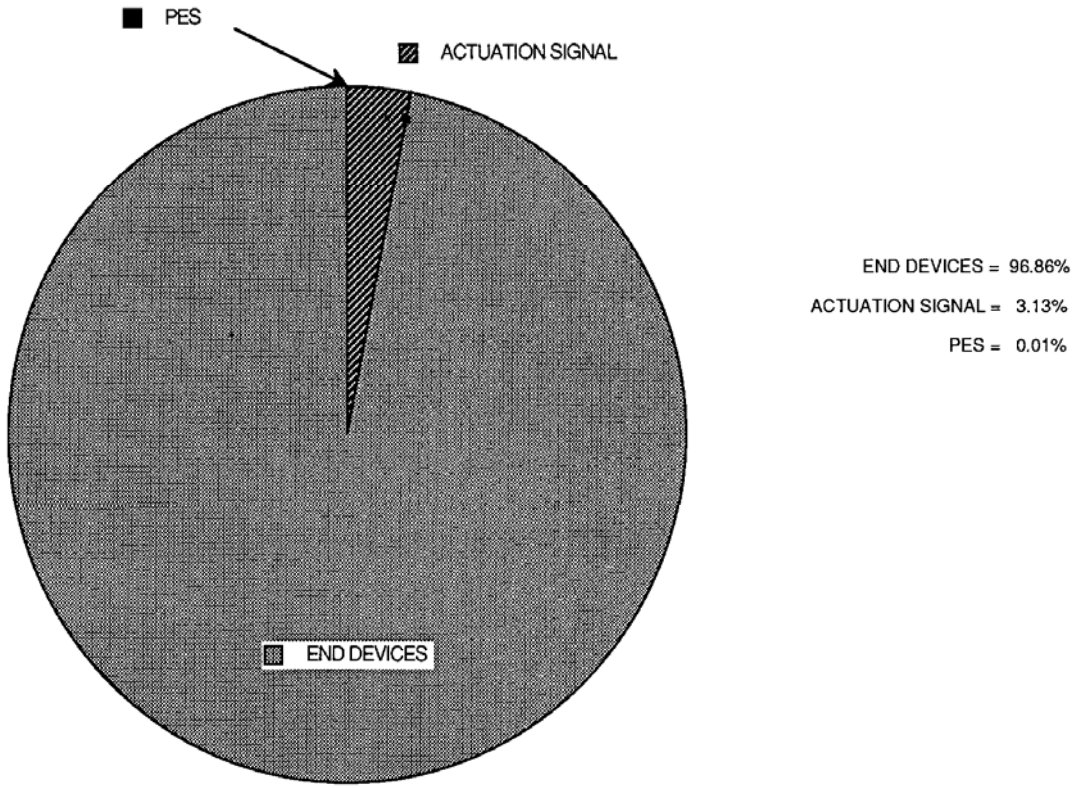


FIGURE 2

COMPARISON OF THE UNAVAILABILITITES OF
DIFFERENT LPU TYPES FOR A TYPICAL TYPE I PLATFORM SHUT-DOWN LOOP
(PRODUCTION HEADER PSL)

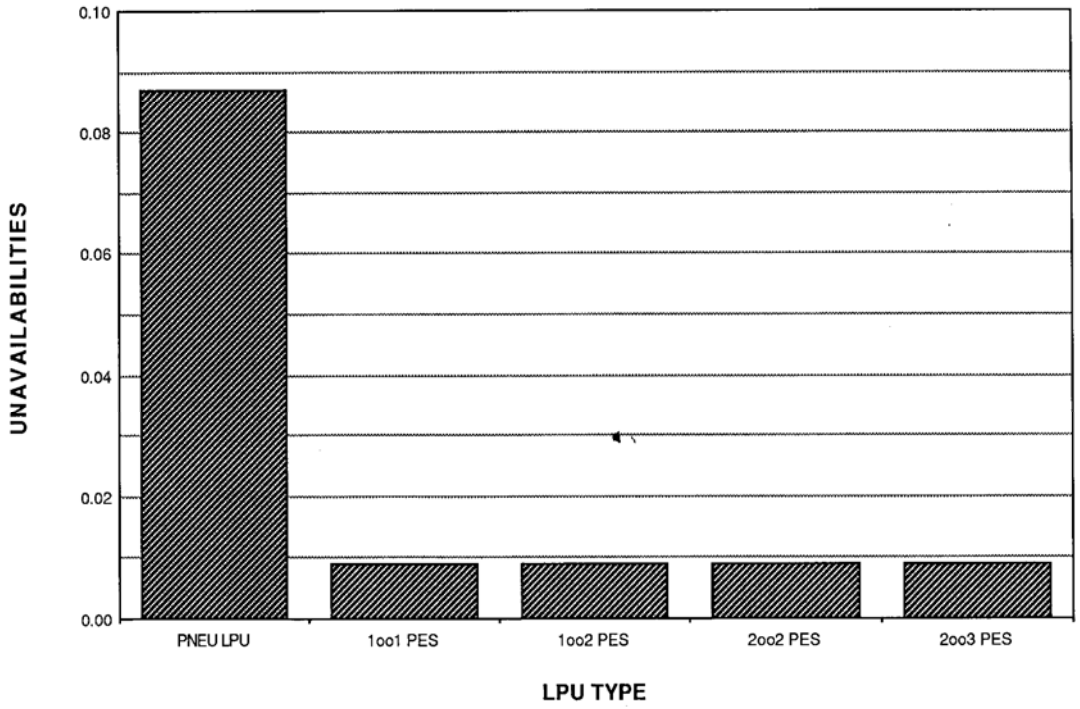
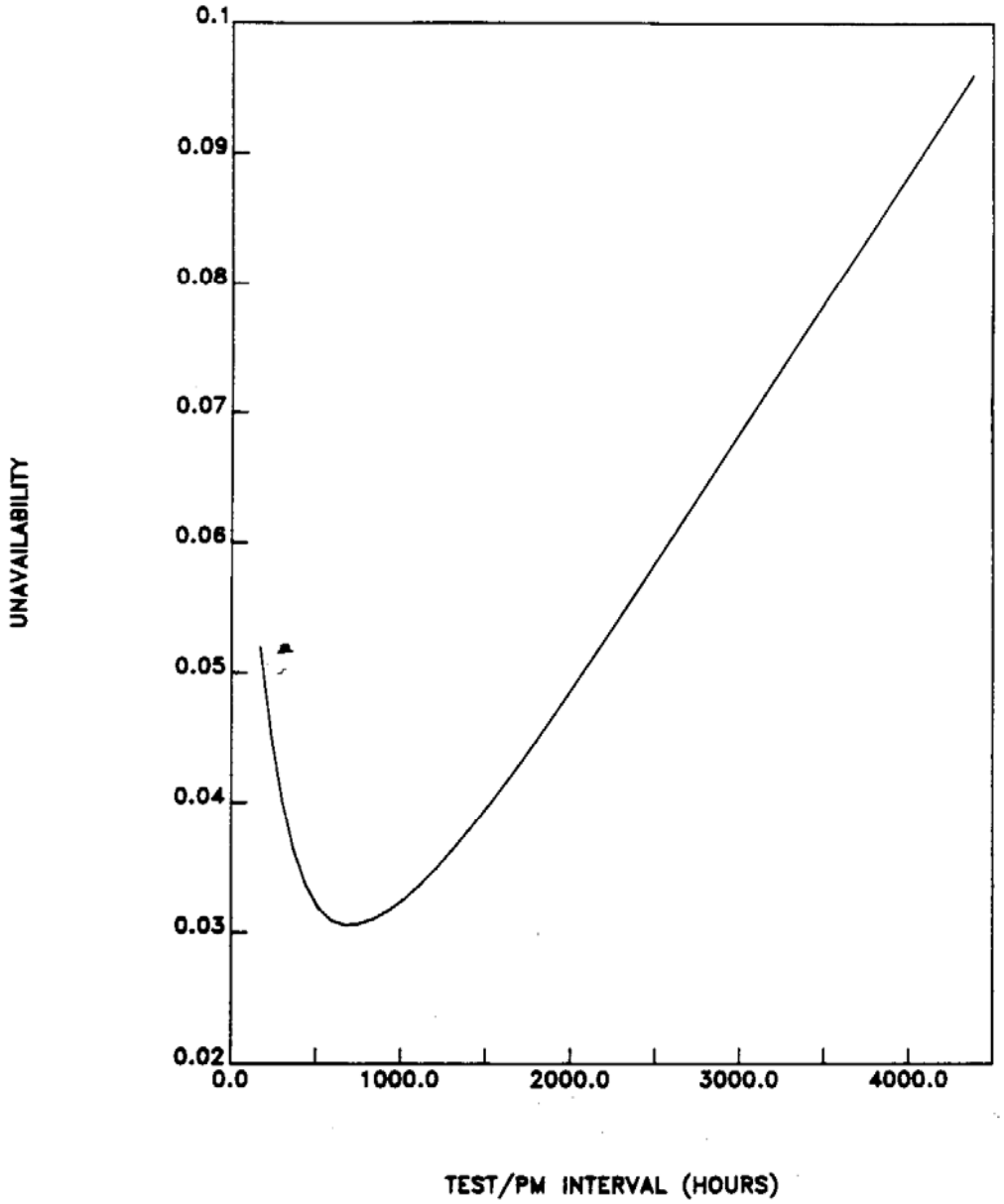


FIGURE 3

MOBIL TYPE I OFFSHORE PLATFORM

UNAVAILABILITY VS. TEST/PM INTERVAL – FIRE/ESD



FIREESD