RISK ASSESSMENT OF THE DEEPWATER HORIZON BLOWOUT PREVENTER (BOP) CONTROL SYSTEM

April 2000 – Final Report

☐ 1. Approved-No Comments
☒ 2. Approved-See Comments
☐ 3. Disapproved-See Comments
☐ 4. Received-No Action Taken

Date Received _____
Received By _____
Date Reviewed 9/12/00
Reviewed By DAC

Houston File Location

NOTE: Drawing approval does not relieve Builder of responsibility to comply with its contractual requirements, to insure compatibility of this drawing with other drawings and to correct any errors or omissions discovered subsequently. All deviations from contractual requirements must be specifically noted as such.

See IDC transmittal Sheet Box Tillison Comment.

Prepared By:

Marc D. Quilici
Eric J. Jorgenson
EQE International
Seattle, Washington

Project #: _____

P.O. #: 087-00101

Comp. #: 139

Prepared for:

CAMERON CONTROLS CORP.
Houston Texas

MAY 1 1 2000

EQE Project Number: 253150

Notice: Proprietary Rights Involved

4120
Exhibit No. _____
Worldwide Court Reporters, Inc.

589604630

TABLE OF CONTENTS

APPENDICES

589604631

1. INTRODUCTION

Cameron Controls is developing and building a blowout preventer (BOP) control system under contract to R & B Falcon Drilling. The BOP is designed for deepwater drilling operations up to 10,000 feet below sea level and is to be installed on the Deepwater Horizon. EQE was contracted by Cameron to conduct a risk assessment of the BOP system. The risk assessment was developed to identify any reliability concerns and rank the contributors to system unavailability based on their likelihood of occurrence.

This report documents the analyses of the Cameron BOP control system to function properly on demand. The analyses were performed using a quantitative method, Fault Tree Analysis.

The fault tree analysis of the BOP control system design uses boolean logic fault tree models which were developed for each of the various portions of the system. The model was evaluated using the SAPHIRE fault tree computer code. The results of this evaluation are an identification of the combinations of equipment failures, operator errors, and/or environmental conditions, which if they occur will lead to failure of the BOP to perform its desired function. Each of these combinations is called a "cutset" and each cutset represent one minimal grouping of failures leading to the undesired failure state.

This quantified fault tree model of the BOP control system also evaluates the probability of failure on demand of the modeled system. This probability of failure is largely site independent, although specific environmental conditions could have some impact on the results. In order for the model to be useful, it is important that the details of the BOP control system configuration be accurately reflected. While generic data for BOP control systems are available in the OREDA database at a high level, a fault tree analysis performed for the specific BOP control system design provides a more accurate picture of system reliability. The results also allow a more detailed exploration of the system design to determine potential weak areas in the design with respect to reliability.

The undesired BOP failure states included in the risk assessment were defined and agreed upon during discussions between Cameron and EQE. These undesired

events form the definition for the fault tree models developed. These events are defined as failure of the system in such a manner as to result in potentially severe environmental damage and/or significant danger to personnel safety. The specific events and subevents examined by the analysis are:

1. Failure to perform the critical functions of the emergency disconnect sequence (EDS) are examined as a single event as well as individually, including:

   - Failure to close the blind shear ram,
   - Failure to close the casing shear ram (if casing is in the stack),
   - Failure to disconnect the riser from the stack,
   - Failure to close the upper and lower choke lines,
   - Failure to close the upper and lower kill lines.

2. Failure to adequately perform well control operations, including:

   - Failure to close the upper and lower annular,
   - Failure to close shear rams and the pipe rams,
   - Failure to open the applicable upper or lower choke lines, or
   - Failure to open the applicable upper or lower kill lines.

The fault tree models and FMEA were developed based on design and operational information provided by R & B Falcon and Cameron Controls. The risk assessment includes:

1) the electro-hydraulic system necessary to perform the EDS and well control functions up to but not including the ship's hydraulic supply to the subsea units;

2) the yellow and blue pod subsea electronic modules, each containing two redundant sets of electronics which control the position of the electro-hydraulic valves;

3) the modems and multiplex cables used to transmit the signals from the surface to the subsea electronic modules;

4) the communication and power distribution cabinets;

5) the Driller's and Toolpusher's control panels;

6) the CCU Workstation;

7) the uninterruptible power supply (UPS) up to but not including the ship's supply buses.

The electro-hydraulic models were developed at the component level of detail, e.g., solenoid operated pilot valve, hydraulic operated inner choke valve, pressure regulators, etc. The electronics portions of the models were typically developed at the board level of detail. All other portions of the model were developed at the component level of detail. Human errors were included in the model for failing to perform various necessary actions such as initiating the emergency disconnect sequence, switching to the backup electronics pod in the event of a failure of the active pod, or actuating individual components in those cases where the EDS is not present.

This report summarizes the development of the fault tree model and the results obtained from its evaluation. Section 2 is a short summary of the fault tree analysis analytical tool. Section 3 provides a specific description of the fault tree model, including the top events developed, the data used to evaluate the model, and key assumptions used in the model development. Section 4 summarizes the results obtained from the fault tree model evaluation. Section 5 provides a summary of observations that can be drawn from the evaluation results. The graphical printout of the fault tree model, the data used in the evaluation, the failure cutset listings, and the importance measure calculations are provided in the appendices in their raw form.

2. FAULT TREE METHODOLOGY

Fault tree analysis is an analytical tool that uses deductive reasoning and a graphical depiction of that reasoning process to determine the various failure event combinations, which if they occur, lead to the occurrence of an undesired event. It is a structured, systematic approach that can be used to evaluate a single system or multiple systems and account for system interactions. Fault tree analysis is a tool that can be used to develop both qualitative and quantitative results.

The fault tree model is developed from logic gates, which are graphic representations of Boolean AND and OR operators, and basic events which are analogous to individual failures. The graphical symbols seen in Figure 2-1 are the symbols most often used in fault tree analysis. These symbols are AND Gate, OR Gate, Transfer, and Basic Event. These symbols and their definitions are discussed below.

OR GATE (SEE SYMBOL LABELED OR-GATE)

A Boolean logic operator with one or more inputs which is true if any of the inputs to the gate are true. For example, in the figure below, if any of the basic events, BASIC-EVENT-2, BASIC-EVENT-3, or BASIC-EVENT-4 which are input to the OR gate occur, the OR gate is considered to occur.

AND GATE (SEE SYMBOL LABELED AND-GATE)

A Boolean logic operator with one or more inputs which is true if all the inputs to the gate are true. For example, in the figure below, if the basic event (labeled BASIC-EVENT-1) and the OR gate occur, the AND gate is considered to occur.

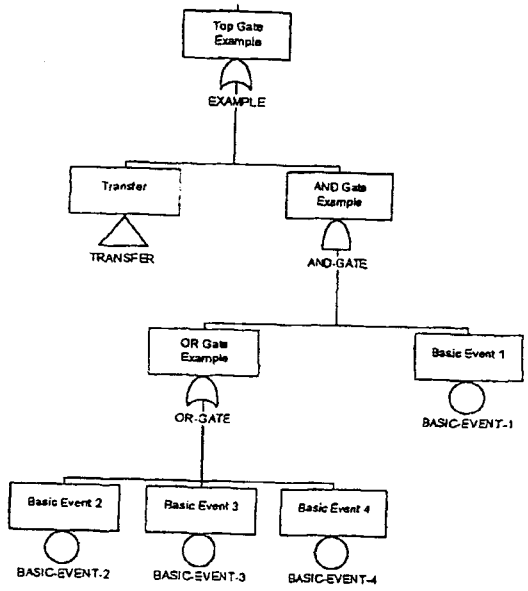


Figure 2-1 - Fault Tree Graphical Symbols

TRANSFER (BOX WITH A TRIANGLE BELOW - SEE SYMBOL LABELED TRANSFER)

Convenience for the analyst which denotes that this event is described in more detail in another place within the model (e.g., another page).

BASIC EVENT (BOX WITH A CIRCLE BELOW - SEE SYMBOLS LABELED BASIC-EVENT-X)

This symbol represents a basic component failure, human error, or maintenance unavailability. These events are representative of the lowest level of resolution in the model. Each basic event has an associated probability of failure associated with it if quantitative results are desired.

589604636

The development of the fault tree model begins by identifying the undesired condition to be examined, commonly referred to as the top event. This event may be defined as broadly or as narrowly as desired but this event definition sets the bounds of the analysis so care must be taken. This event is usually defined as failure to achieve a desired goal for example, "Failure to perform an emergency disconnect". Once the top event is defined, the analyst performs a systematic review of each small piece of the system to determine how that event can happen, either in terms of basic events (e.g., Failure of the upper shear ram to shear the pipe) or in terms of other broader events (e.g., Failure of hydraulic supply to the upper shear ram). These broadly defined events are usually represented by AND or OR logic gates which are then examined in the same manner as the top event. The modeling process continues until all of the broad events are defined in terms of basic events and the associated logic gates. The fault tree logic model is then evaluated to determine the possible combinations of basic events that will result in occurrence of the top event. These possible combinations are referred to as cutsets. The cutsets may be qualitative in nature if no failure data is applied or quantitative if failure data is applied depending upon the desired goal of the analysis.

3. FAULT TREE ANALYSIS

The fault tree model was developed to represent system functions that are required to successfully shut-in the well and disconnect the LMRP. These functions are included in the EDS and are intended to ensure personnel safety and isolation of the well to preserve the environment. Well control functions, including operation of choke and kill valves and the hydraulic supplies for closure of the upper and lower annulars and the shear and pipe rams were also modeled.

Systems, equipment and components that are necessary to accomplish an EDS were modeled from the individual hydraulic supplies to the BOP Stack components back through the entire system to the ship electrical and hydraulic supply. Estimated failure rates were included in the model to achieve an understanding of the relative importance of failure combinations. Reliability of operators, where human actions are necessary, was also modeled. Common cause failures (CCFs) are failures which, as the name implies, arise from common causes. Since these events have historically been found to occur with a higher likelihood of occurrence than independent failures of similar components, they tend to become important in highly redundant systems. In this modeling effort, CCFs were included in the model for failures of CPU boards, fuses, modems, and power supplies. These CCFs were postulated for multiple identical components that are in similar environments. For example, CCFs were included for failure of both CPU boards in a single pod and for failure of all four CPU boards in the blue and yellow pods. No CCFs were included for components which are in different physical locations and environments. Although a case may be made for some potential for CCFs in these cases, they are in non-redundant sets of components within the same signal flow path and therefore do not significantly affect the system reliability.

In order to focus on the equipment necessary to perform the EDS and Well Control operations, simplified block diagrams were developed for the electronic portions of the system. These block diagrams were developed from the detailed electrical schematics for the Driller's Panel, the Toolpusher's Panel, the CCU Workstation, the Communication/Power Distribution Cabinets, and the Subsea Electronic Modules and their accuracy was verified by the applicable Cameron personnel. The block diagram representations of the electronic portion of the control system formed the

basis for the fault tree model and are shown in Figures 3-1 through 3-11. Table 3-1 identifies the modeled configuration for solenoid/connector assumed assignments.

A description of fault tree top logic, model assumptions, and input data are discussed in Sections 3.1, 3.2, and 3.3, respectively.

3.1 TOP LOGIC

Top logic for the fault tree was defined based on the successful operation of an EDS: closure of the upper or lower shear ram, riser disconnect, opening the upper annular, and isolation of the choke and kill valves. Closure of the upper or lower shear ram will isolate the riser as well as cut the drill string for separation from the BOP Stack. Riser disconnect will allow separation of the riser from the stack. Opening of the upper annular will facilitate separation of the riser (and drill ship) from the stack. Isolation of the Choke and Kill lines along with closure of the shear ram will isolate the well to prevent the release of well contents to the environmental. These same functions are also modeled in a top logic model for a planned disconnect.

The probability of successful operation of these functions is modeled by the following failure to operate BOP fault tree top logic:

- Failure to close the blind shear ram
- Failure to close the casing shear ram if casing is present
- Failure to disconnect the riser from the stack
- Failure to isolate the upper and lower choke lines
- Failure to isolate the upper and lower kill lines

A separate model top logic was developed to evaluate the probability of failure of the essential well control functions and consisted of the following:

- Failure to close the blind shear ram, or failure to open the upper or lower choke lines or the upper or lower kill lines, or close the upper and lower annulars
- Failure to close the pipe rams, or failure to open the available upper or lower choke lines and the upper or lower kill lines, or close the upper and lower annulars

3.2 ASSUMPTIONS

Generation of fault tree models in order to gain a quantitative understanding of the system reliability and governing failure combinations, required a number of important assumptions. Assumptions were established during development of the model based on the following:

- Definition of Undesired Events
- System Operational Functional Description
- Inputs/Outputs for Each Component
- System Design/Operational Requirements
- Monitored Parameters and Associated Instrumentation Which Identify Need for Actuation
- Maintenance/Testing Practices, Frequencies, and Philosophies

The above information was compiled based on hydraulic, electrical, instrumentation, and control system drawings as well as interviews with R&B Falcon and Cameron staff. Access to information from the Cameron Project Manager and engineers responsible for various aspects of the system was provided to the analysis team.

Resulting key model boundary conditions and assumptions follow:

1. EDS failure is defined as failure to close blind shear ram or failure to close the casing shear ram when casing is in the hole or failure to disconnect riser or failure to open upper annular or failure to isolate choke or failure to isolate kill.

2. Well control failure is defined as failure to seal using the blind shear ram or any one of the three pipe rams or failure to open any applicable choke or kill paths or failure to close the upper and lower annular.

3. The EDS1 and EDS2 sequences are taken into account in the model by accounting for the fraction of the time that casing or a tool joint is in the stack. The human error for failure to initiate EDS is considered to include the proper mode selection. An estimate of 5% of the time was made that the casing shear ram is required. This estimate is felt to be conservative.

4. The casing shear ram is not considered to be a redundancy to the blind shear ram due to its inability to seal the well in.

5. It is assumed that the pressure regulators do not require either an increase or decrease signal during the period of operation of critical functions.

6. It is assumed that the stack accumulator charge signal is active during normal pod operation.

7. Unlock of the choke and kill connectors is not required for successful riser disconnect.

8. Closure of the inner and outer bleed valves is not required for successful EDS.

9. All components are assumed to be designed with sufficient margin, and of sufficient quality, ("i.e., "fit for service") to fit their intended applications.

10. Although retraction of stabs is a desirable function to avoid hardware damage, retraction was not included in the model because failure of retraction would not prevent disconnect and there would be no significant personnel or environmental hazard associated with failure.

11. Closure of the choke and kill isolation valves are not required for successful EDS operation.

12. The blue pod is normally in operation and the yellow pod is in standby. Although pod operation is rotated on a weekly basis, the model was developed for one configuration. Due to symmetry between the pods, the results are not impacted with the exception of the dominance of blue pod components. The importance of each failure identified associated with the blue pod components is equivalent for the yellow pod.

13. Failures associated with the cable reels are assumed to be covered in the cabling.

14. Since it is allowable to continue drilling with one train of POD electronics unavailable due to failures it is important to account for these partial failures. An overall POD electronics train unavailability due to prior failure is estimated to be 3.3E-1/drilling operation (1 failure in 3 drilling operations) in order to account

for the potential operation with one train of electronics failed within a POD. This is estimated by a failure rate of 3.18E-5/hr * 21 components * 45 days/drilling operation.

15. Failure of the "deadman" system (DMS) is conservatively not modeled for EDS. Spurious operation is considered to be statistically negligible based on the number of required failures necessary for spurious operation.

16. The solenoid cables to be used in the system are assumed to be "fit for purpose" and are not included in the model due to low cable failure rates for appropriate cable and the limited impact of single failures.

17. The pod bulkhead connectors are assumed to be more likely to leak with one or more of the pie connector plugs disconnected due to the lower open face pressure rating of the connector.

18. Failure of an isometer in one of the Communication/Power Distribution Panels can only isolate one pod.

19. The CCU workstation was not modeled in detail due to a lack of design information. The communication with the CCU Workstation was modeled however.

20. Both the blue and yellow hydraulic signals for opening the blue and yellow pod hot line supplies are always active.

21. If both the open and close (latch and unlatch) pilot signals are applied to a three position hydraulic operated valve, the actual position is indeterminate and the valve is assumed to fail.

22. The hot lines are assumed to be a redundancy to the rigid conduit for hydraulic supply. Although the operation of components will be slower, all the required functions can be operated and the largest consumers also have accumulator back up.

23. The upper and lower annular are completely redundant for well control operations.

3.3 DATA

Fault trees were developed using the computer code SAPHIRE, a risk analysis software package developed by Idaho National Engineering Laboratory (INEL) contractors for probabilistic analyses of nuclear power and nuclear weapons facilities. The resulting model includes almost 1800 logic gates and approximately 750 basic events.

Failure rates were assigned to the basic events based on the OREDA-92 and OREDA-97 offshore reliability databases, a combination of published data compiled for the nuclear industry, published data compiled for military applications, discussion with Cameron engineers, experience of the analysts, and engineering judgment.

Where available and in sufficient detail, data from the OREDA databases was preferentially used. In some cases however, either the data was unavailable for specific components or the data could not be broken down to the model level of detail. In these cases, other published data was used to estimate failure rates for components that are similar in type and function to standard hardware (solenoid valves, hydraulic valves, cable, etc.). It is recognized that hardware designed for the BOP service environment is not typical of industrial or military grade equipment. Although the service conditions for the subsea components is severe, many design features have been added to minimize the potential for environmental conditions to impact the reliability of the BOP. These data sources are therefore considered.

Most of the component failure rates used in the quantification of the overall failure probability are time-dependent. Most of the components are in the standby state during the majority of the drilling operation. The component failure probabilities for standby components with periodic testing are calculated from the following equation:

$$P = 1 + (e^{[-\lambda\tau]} - 1) / (\lambda\tau)$$

Where: λ = time dependent failure rate

τ = test interval

The test intervals associated with the various components were based on an estimate of how often the components would be demonstrated to be operable. In general, 4 time periods were used. Main power supply breakers and transformers would be expected to be monitored continuously and are assigned a test interval of 1 hour, which is conservative. Components such as the rams are tested weekly and are assigned a test interval of 168 hours. Electronic components associated with the operating and standby pod are continuously monitored and are assigned a conservative test interval of 1 hour. Components associated with the standby pod which are not continuously monitored are assigned a test interval of 168 hours (1 week) based on the expected weekly rotation of operational pods. Components which would be tested only by an actual disconnect were assigned a 1000 hour test interval, estimating a conservative average of one planned and one unplanned disconnect per drilling operation. The UPS batteries are only needed if power is lost and therefore may only be infrequently load tested. The batteries are therefore assigned a test interval of 2920 hours (1/3 year).

Experience and judgment was the primary method for estimating failure rates for components with limited failure data (such as modems, optical link modules, workstations, and software). In such cases, conservative failure rates were entered to determine the overall effect on system reliability.

Failure rates for operators to take necessary actions were estimated based on all of the above, with sensitivity studies performed to gain an understanding of the importance of operator actions. Experience, training, and system indication are key elements to reliable operator actions.

Common cause events were quantified using the multiple greek letter (MGL) method. Based on the data in OREDA-97 for control logic units, approximately 7% of the failures were attributable to common cause failures. This was used as the beta factor, which when multiplied by the individual component failure rate estimates the likelihood of two similar components to fail due to a common cause. No data regarding the likelihood of more than two components to fail due to the same common cause is identified in the OREDA data. Based on experience gained

in the nuclear power industry, common cause failures of more than two components actually have occurred and have resulted in a significant contribution to overall unavailability. The likelihood of failure of a third similar component due to a common cause given failure of two components (delta) is estimated typically to be in the 20-30% range. For common mode failure of four or more components, given failure of three components due to a common mode (gamma), the estimate is typically in the 70-80% range. The failure of more than four components due to common causes given failure of four similar components due to common causes are typically assumed to be 100%. The specific details of the developed factors are shown in Table B-2 in Appendix B.

Basic events were named according to the convention AAA-BBB-CC-ZZZZZ where AAA is the system designator, BBB is the component type, CC is the failure mode, and ZZZZZ is a designator assigned to uniquely identify each event. A listing of basic events along with failure rates for each event are listed in Appendix B.

Table 3-1: Function/Connector Assignments							
No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
1	A	A4	A5	X19	1	A	85 - UIK Open
2	A	A4	A5	X19	1	B	86 - UIK Close
3	A	A4	A5	X19	1	C	87 - LOK Open
4	A	A4	A5	X19	1	D	88 - LOK Close
5	A	A4	A5	X19	1	E	
6	A	A4	A5	X19	1	F	
7	A	A4	A5	X20	2	A	
8	A	A4	A5	X20	2	B	
9	A	A4	A6	X20	2	C	
10	A	A4	A6	X20	2	D	
11	A	A4	A6	X20	2	E	
12	A	A4	A6	X20	2	F	
13	A	A4	A6	X21	3	A	
14	A	A4	A6	X21	3	B	12 - UA Preventer Close
15	A	A4	A6	X21	3	C	
16	A	A4	A6	X21	3	D	14 - LA Preventer Close
17	A	A7	A8	X21	3	E	15 - Blue Pod Hot Line Supply Open
18	A	A7	A8	X21	3	F	
19	A	A7	A8	X23	4	A	49 - Pod Select Pilot Open
20	A	A7	A8	X23	4	B	
21	A	A7	A8	X23	4	C	

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
22	A	A7	A8	X23	4	D	
23	A	A7	A8	X23	4	E	31 - LMRP Conn. Secondary Unlatch
24	A	A7	A8	X23	4	F	
25	A	A7	A9	X24	5	A	
26	A	A7	A9	X24	5	B	
27	A	A7	A9	X24	5	C	
28	A	A7	A9	X24	5	D	
29	A	A7	A9	X24	5	E	
30	A	A7	A9	X24	5	F	
31	A	A7	A9	X25	6	A	
32	A	A7	A9	X25	6	B	
33	A	A10	A11	X25	6	C	
34	A	A10	A11	X25	6	D	
35	A	A10	A11	X25	6	E	
36	A	A10	A11	X25	6	F	
37	A	A10	A11	X27	7	A	
38	A	A10	A11	X27	7	B	
39	A	A10	A11	X27	7	C	
40	A	A10	A11	X27	7	D	
41	A	A10	A12	X27	7	E	
42	A	A10	A12	X27	7	F	

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
43	A	A10	A12	X28	8	A	
44	A	A10	A12	X28	8	B	
45	A	A10	A12	X28	8	C	
46	A	A10	A12	X28	8	D	
47	A	A10	A12	X28	8	E	103 - HP Shear Close
48	A	A10	A12	X28	8	F	
49	A	A13	A14	X30	9	A	95 - LOC Open
50	A	A13	A14	X30	9	B	96 - LOC Close
51	A	A13	A14	X30	9	C	97 - LIC Open
52	A	A13	A14	X30	9	D	98 - LIC Close
53	A	A13	A14	X30	9	E	99 - HP Casing Shear Close
54	A	A13	A14	X30	9	F	
55	A	A13	A14	X31	10	A	91 - UOC Open
56	A	A13	A14	X31	10	B	92 - UOC Close
57	A	A13	A15	X31	10	C	
58	A	A13	A15	X31	10	D	76 - Upper Pipe Ram Close
59	A	A13	A15	X31	10	E	
60	A	A13	A15	X31	10	F	78 - Middle Pipe Ram Close
61	A	A13	A15	X32	11	A	
62	A	A13	A15	X32	11	B	
63	A	A13	A15	X32	11	C	
64	A	A13	A15	X32	11	D	

BAE

589604648

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
65	A	A16	A17	X32	11	E	
66	A	A16	A17	X32	11	F	66 - Shearing Blind Ram #1 Close
67	A	A16	A17	X34	12	A	
68	A	A16	A17	X34	12	B	68 - Lower Pipe Ram #5 Close
69	A	A16	A17	X34	12	C	
70	A	A16	A17	X34	12	D	
71	A	A16	A17	X34	12	E	
72	A	A16	A17	X34	12	F	72 - Casing Shear Ram #2 Close
73	A	A16	A18	X35	13	A	
74	A	A16	A18	X35	13	B	
75	A	A16	A18	X35	13	C	
76	A	A16	A18	X35	13	D	82 - Stack Accumulator Charge
77	A	A16	A18	X35	13	E	83 - UOK Open
78	A	A16	A18	X35	13	F	84 - UOK Close
79	A	A16	A18	X36	14	A	17 - LMRP Connector Unlatch
80	A	A16	A18	X36	14	B	
81	A	A19	A20	X36	14	C	
82	A	A19	A20	X36	14	D	
83	A	A19	A20	X36	14	E	23 - LMRP Accumulator Charge
84	A	A19	A20	X36	14	F	
85	A	A19	A20	X38	15	A	

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
86	A	A19	A20	X38	15	B	
87	A	A19	A20	X38	15	C	
88	A	A19	A20	X38	15	D	
89	A	A19	A21	X38	15	E	29 - Yellow Pod Hot Line Supply Open
90	A	A19	A21	X38	15	F	
91	A	A19	A21	X39	16	A	89 - LIK Open
92	A	A19	A21	X39	16	B	90 - LIK Close
93	A	A19	A21	X39	16	C	42 - Yellow Pod Conduit Supply Open
94	A	A19	A21	X39	16	D	43 - Blue Pod Conduit Supply Open
95	A	A19	A21	X39	16	E	93 - UIC Open
96	A	A19	A21	X39	16	F	94 - UIC Close
97	A	A22	A23	X41	17	A	
98	A	A22	A23	X41	17	B	
99	A	A22	A23	X41	17	C	
100	A	A22	A23	X41	17	D	
101	A	A22	A23	X41	17	E	
102	A	A22	A23	X41	17	F	
103	A	A22	A23	X42	18	A	
104	A	A22	A23	X42	18	B	
105	A	A22	A24	X42	18	C	

BOE

589604650

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn No.	Plug	Horizon Component Signal
106	A	A22	A24	X42	18	D	
107	A	A22	A24	X42	18	E	
108	A	A22	A24	X42	18	F	
109	B	A35	A36	X19	1	A	85 - UIK Open
110	B	A35	A36	X19	1	B	86 - UIK Close
111	B	A35	A36	X19	1	C	87 - LOK Open
112	B	A35	A36	X19	1	D	88 - LOK Close
113	B	A35	A36	X19	1	E	
114	B	A35	A36	X19	1	F	
115	B	A35	A36	X20	2	A	
116	B	A35	A36	X20	2	B	
117	B	A35	A37	X20	2	C	
118	B	A35	A37	X20	2	D	
119	B	A35	A37	X20	2	E	
120	B	A35	A37	X20	2	F	
121	B	A35	A37	X21	3	A	
122	B	A35	A37	X21	3	B	12 - UA Preventer Close
123	B	A35	A37	X21	3	C	
124	B	A35	A37	X21	3	D	14 - LA Preventer Close
125	B	A38	A39	X21	3	E	15 - Blue Pod Hot Line Supply Open
126	B	A38	A39	X21	3	F	

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
127	B	A38	A39	X23	4	A	49 - Pod Select Pilot Open
128	B	A38	A39	X23	4	B	
129	B	A38	A39	X23	4	C	
130	B	A38	A39	X23	4	D	
131	B	A38	A39	X23	4	E	31 - LMRP Conn. Secondary Unlatch
132	B	A38	A39	X23	4	F	
133	B	A38	A40	X24	5	A	
134	B	A38	A40	X24	5	B	
135	B	A38	A40	X24	5	C	
136	B	A38	A40	X24	5	D	
137	B	A38	A40	X24	5	E	
138	B	A38	A40	X24	5	F	
139	B	A38	A40	X25	6	A	
140	B	A38	A40	X25	6	B	
141	B	A41	A42	X25	6	C	
142	B	A41	A42	X25	6	D	
143	B	A41	A42	X25	6	E	
144	B	A41	A42	X25	6	F	
145	B	A41	A42	X27	7	A	
146	B	A41	A42	X27	7	B	
147	B	A41	A42	X27	7	C	

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
148	B	A41	A42	X27	7	D	
149	B	A41	A43	X27	7	E	
150	B	A41	A43	X27	7	F	
151	B	A41	A43	X28	8	A	
152	B	A41	A43	X28	8	B	
153	B	A41	A43	X28	8	C	
154	B	A41	A43	X28	8	D	
155	B	A41	A43	X28	8	E	103 - HP Shear Close
156	B	A41	A43	X28	8	F	
157	B	A44	A45	X30	9	A	95 - LOC Open
158	B	A44	A45	X30	9	B	96 - LOC Close
159	B	A44	A45	X30	9	C	97 - LIC Open
160	B	A44	A45	X30	9	D	98 - LIC Close
161	B	A44	A45	X30	9	E	99 - HP Casing Shear Close
162	B	A44	A45	X30	9	F	
163	B	A44	A45	X31	10	A	91 - UOC Open
164	B	A44	A45	X31	10	B	92 - UOC Close
165	B	A44	A46	X31	10	C	
166	B	A44	A46	X31	10	D	76 - Upper Pipe Ram Close
167	B	A44	A46	X31	10	E	
168	B	A44	A46	X31	10	F	78 - Middle Pipe Ram Close
169	B	A44	A46	X32	11	A	

Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
170	B	A44	A46	X32	11	B	
171	B	A44	A46	X32	11	C	
172	B	A44	A46	X32	11	D	
173	B	A47	A48	X32	11	E	
174	B	A47	A48	X32	11	F	66 - Shearing Blind Ram #1 Close
175	B	A47	A48	X34	12	A	
176	B	A47	A48	X34	12	B	68 - Lower Pipe Ram #5 Close
177	B	A47	A48	X34	12	C	
178	B	A47	A48	X34	12	D	
179	B	A47	A48	X34	12	E	
180	B	A47	A48	X34	12	F	72 - Casing Shear Ram #2 Close
181	B	A47	A49	X35	13	A	
182	B	A47	A49	X35	13	B	
183	B	A47	A49	X35	13	C	
184	B	A47	A49	X35	13	D	82 - Stack Accumulator Charge
185	B	A47	A49	X35	13	E	83 - UOK Open
186	B	A47	A49	X35	13	F	84 - UOK Close
187	B	A47	A49	X36	14	A	17 - LMRP Connector Unlatch
188	B	A47	A49	X36	14	B	
189	B	A50	A51	X36	14	C	
190	B	A50	A51	X36	14	D	

BOE

589604654

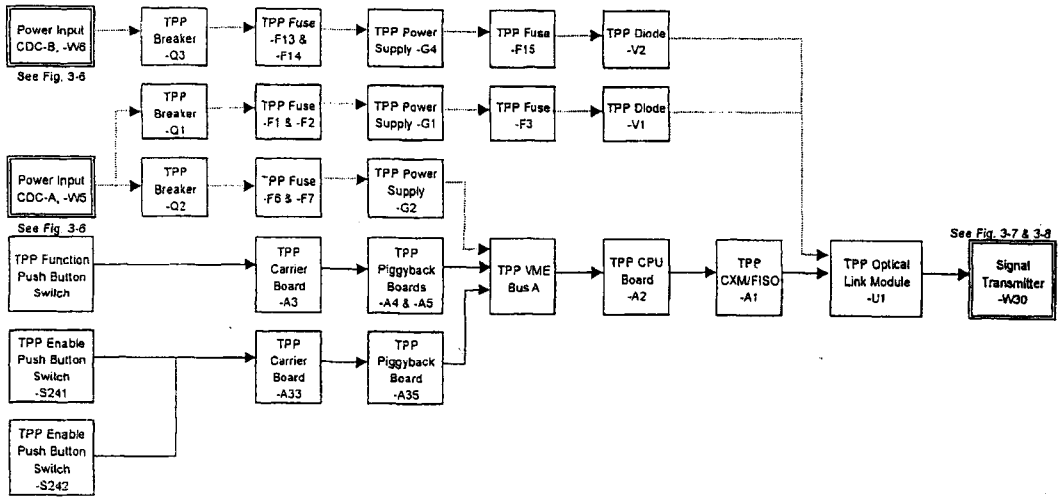
Table 3-1: Function/Connector Assignments

No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
191	B	A50	A51	X36	14	E	23 - LMRP Accumulator Charge
192	B	A50	A51	X36	14	F	
193	B	A50	A51	X38	15	A	
194	B	A50	A51	X38	15	B	
195	B	A50	A51	X38	15	C	
196	B	A50	A51	X38	15	D	
197	B	A50	A52	X38	15	E	29 - Yellow Pod Hot Line Supply Open
198	B	A50	A52	X38	15	F	
199	B	A50	A52	X39	16	A	89 - LIK Open
200	B	A50	A52	X39	16	B	90 - LIK Close
201	B	A50	A52	X39	16	C	42 - Yellow Pod Conduit Supply Open
202	B	A50	A52	X39	16	D	43 - Blue Pod Conduit Supply Open
203	B	A50	A52	X39	16	E	93 - UIC Open
204	B	A50	A52	X39	16	F	94 - UIC Close
205	B	A53	A54	X41	17	A	
206	B	A53	A54	X41	17	B	
207	B	A53	A54	X41	17	C	
208	B	A53	A54	X41	17	D	
209	B	A53	A54	X41	17	E	
210	B	A53	A54	X41	17	F	

Table 3-1: Function/Connector Assignments

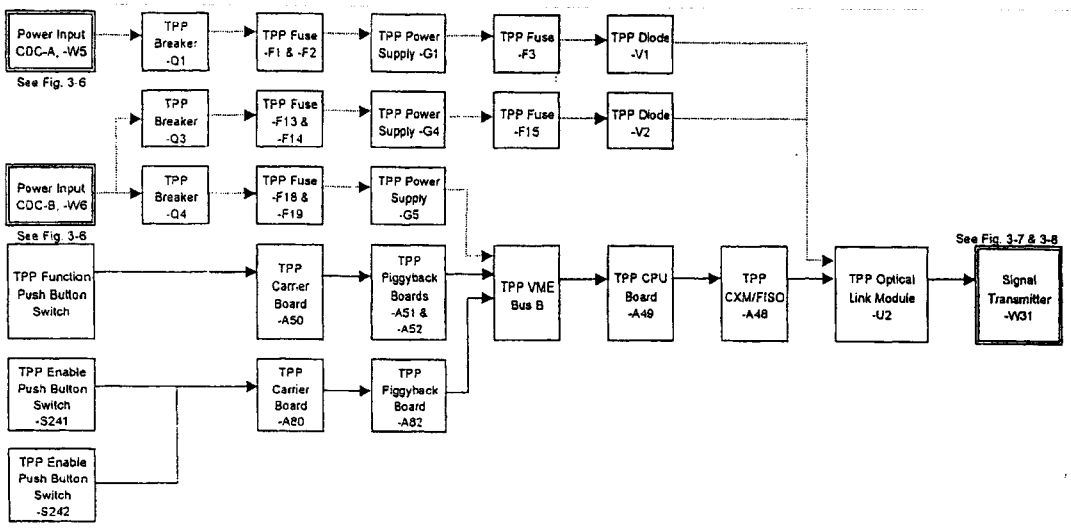
No.	Train	Carrier Board (X)	Piggyback Board (Y)	Connector (Z)	Conn. No.	Plug	Horizon Component Signal
211	B	A53	A54	X42	18	A	
212	B	A53	A54	X42	18	B	
213	B	A53	A55	X42	18	C	
214	B	A53	A55	X42	18	D	
215	B	A53	A55	X42	18	E	
216	B	A53	A55	X42	18	F	

Figure 3-1: General Channel - Toolpusher's Panel (TPP) to Comm./Power Dist. Panel A
From Pushbutton Switch to Transmit Command Signal to CDC



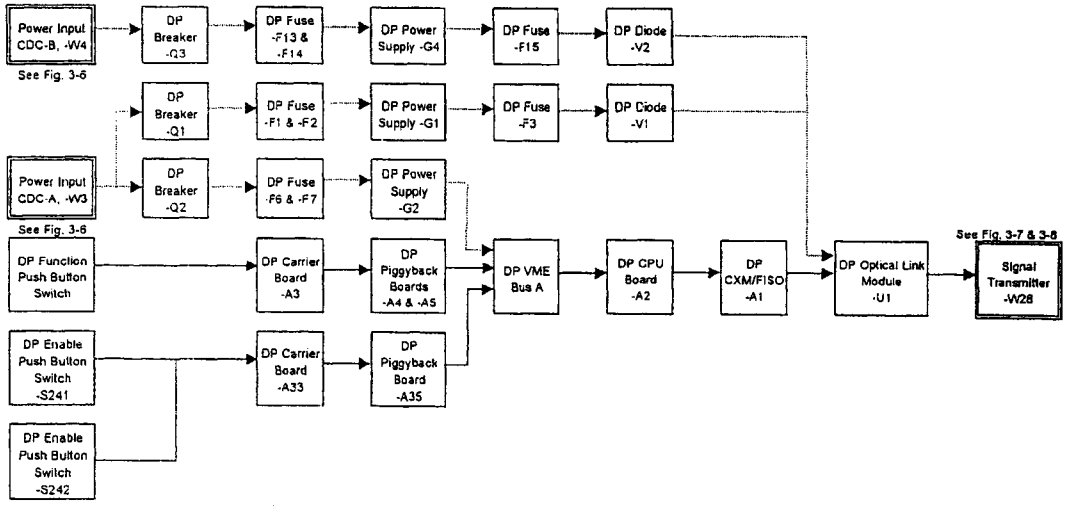
Note: See Figure 3-1 for symbol Key

Figure 3-2: General Channel - Toolpusher's Panel (TPP) to Comm./Power Dist. Panel B
From Pushbutton Switch to Transmit Command Signal to CDC



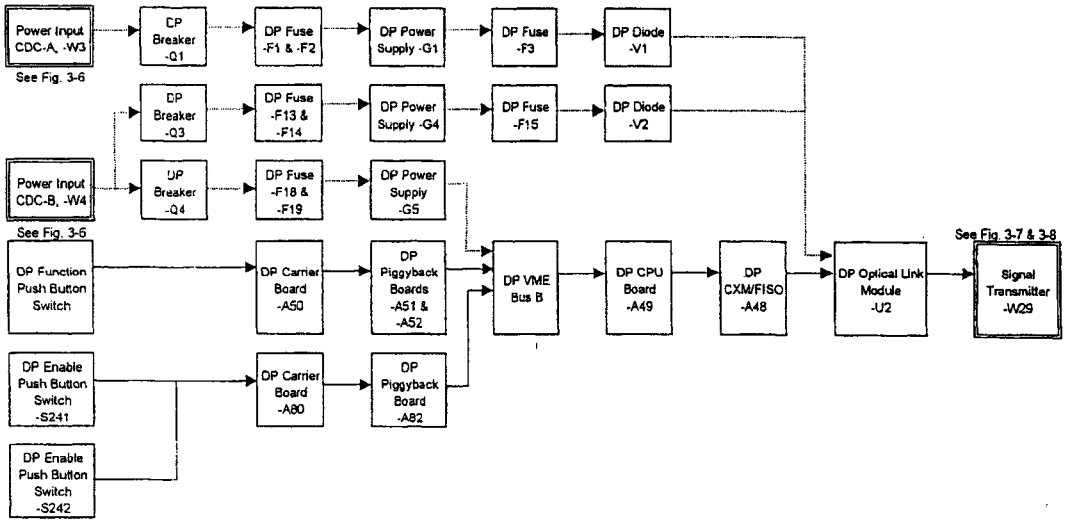
Note: See Figure 3-11 for symbol Key

Figure 3-3: General Channel - Driller's Panel (DP) to Comm./Power Dist. Panel A From Pushbutton Switch to Transmit Command Signal to CDC



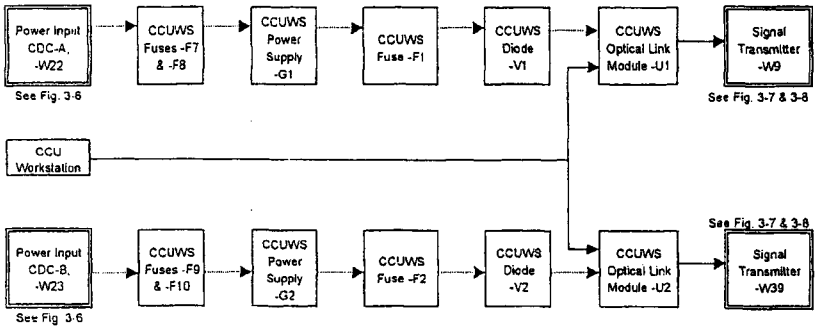
Note: See Figure 3-11 for symbol Key

Figure 3-4: General Channel - *Driller's Panel (DP)* to Comm./Power Dist. Panel B
From Pushbutton Switch to Transmit Command Signal to CDC



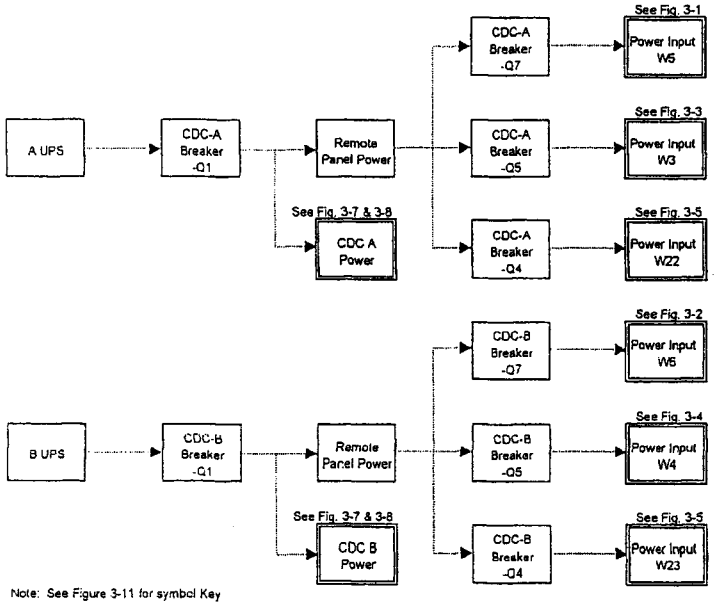
Note: See Figure 3-11 for symbol Key

Figure 3-5: General Channel - CCU Workstation to Comm./Power Dist. Panel A & B
From CCU to Transmit Command Signal to CDC



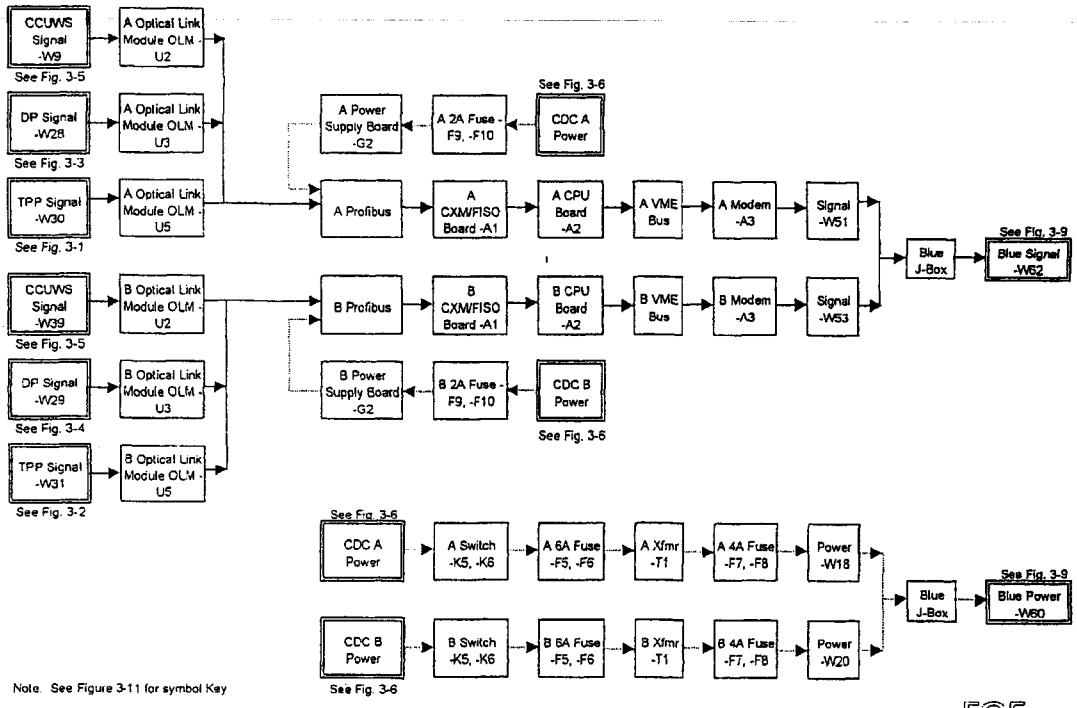
Note: See Figure 3-11 for symbol Key

Figure 3-6: Power - Communications/Power Distribution Panel
Panel A (W5) and B (W6) to Toolpusher's Panel
Panel A (W3) and B (W4) to Driller's Panel
Panel A (W22) and B (W23) to CCU Workstation



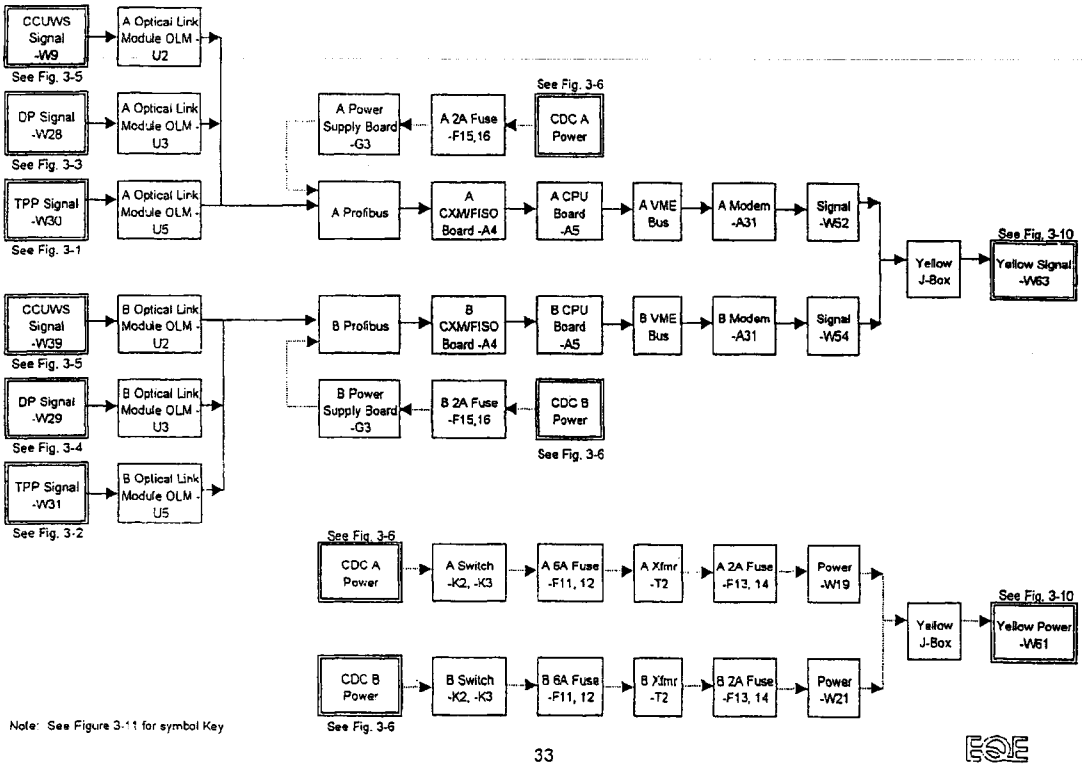
Note: See Figure 3-11 for symbol Key

Figure 3-7: Blue Power/Signal Comm./Power Dist. Panel A&B to -W60, -W62



Note. See Figure 3-11 for symbol Key

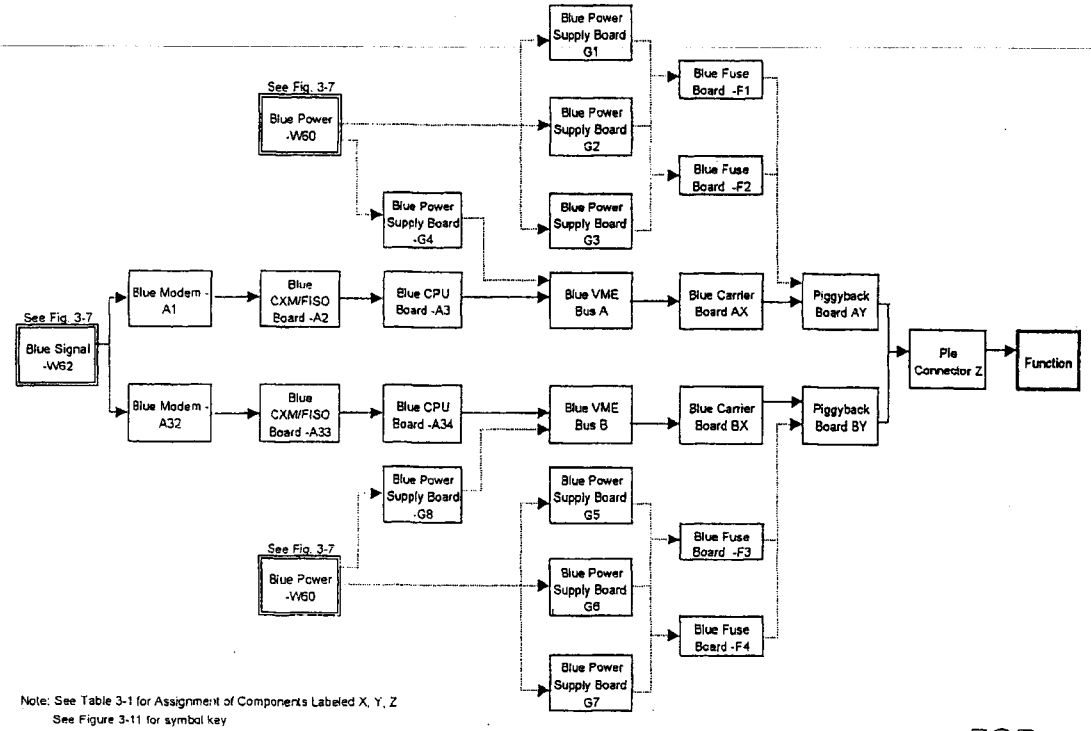
Figure 3-8: Yellow Power/Signal Comm./Power Dist. Panel A&B to -W61, -W63



Note: See Figure 3-11 for symbol Key

5896046691

Figure 3-9: Blue Signal -W62 Thru SEM to Solenoid

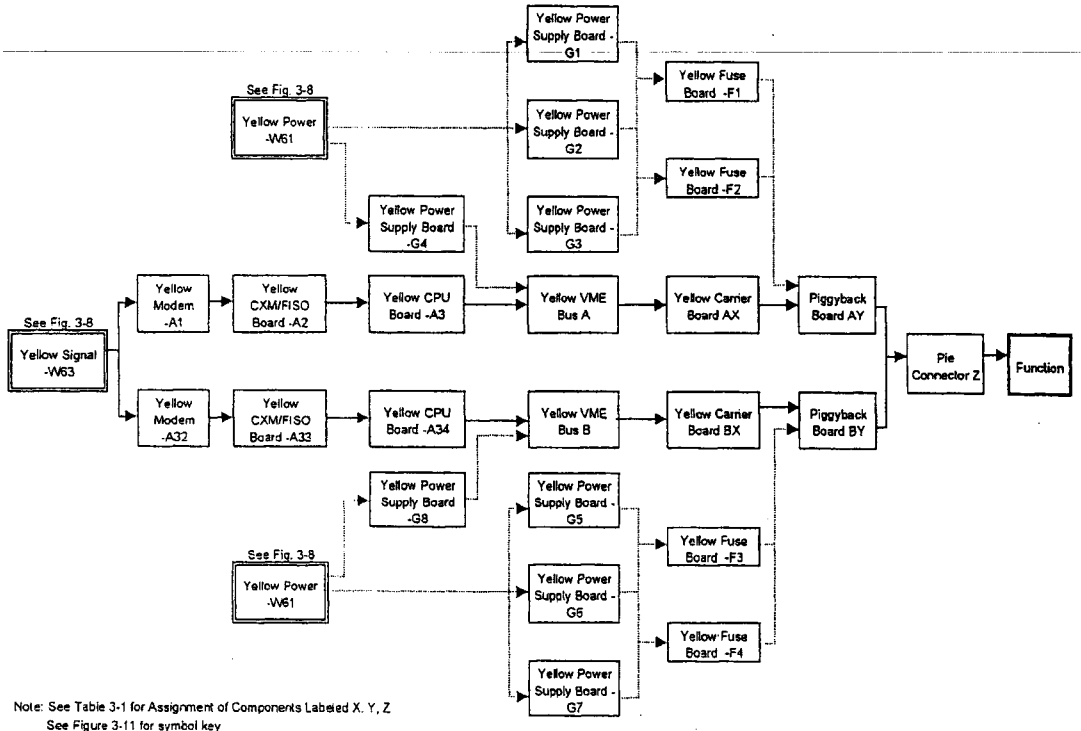


Note: See Table 3-1 for Assignment of Components Labeled X, Y, Z
See Figure 3-11 for symbol key

ESE

5596046

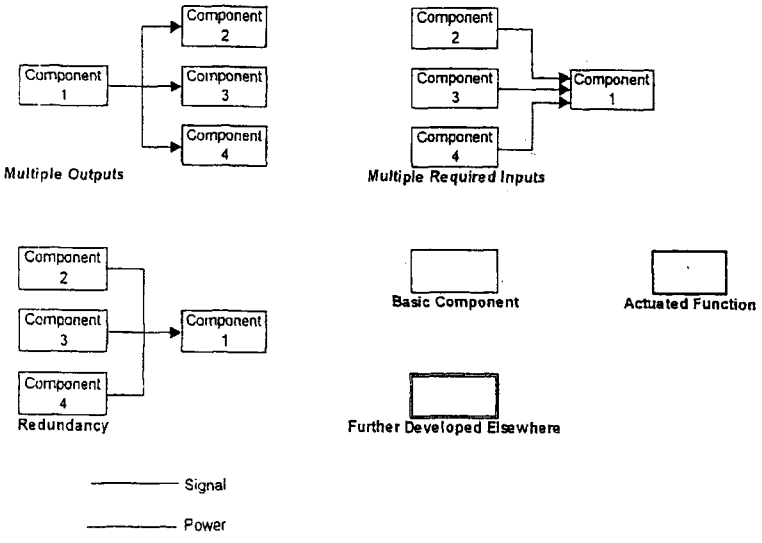
Figure 3-10: Yellow Signal -W63 Thru SEM to Solenoid



Note: See Table 3-1 for Assignment of Components Labeled X, Y, Z
See Figure 3-11 for symbol key

5896046666

Figure 3-11: Flow Diagram Symbol Key



4. EVALUATION RESULTS

As discussed in the introduction, the evaluation of the fault trees by boolean reduction results in the identification of the minimal cutsets, or the minimum combinations of failures that will result in the occurrence of the undesired event. Each of these cutsets is composed of one or more failures and each of the failures is assigned a probability of failure as discussed in Section 3. The product of the failure probabilities for all failure events in a cutset represents the probability of occurrence of the cutset. The sum of the cutsets for each fault tree model represents the probability of occurrence of the associated undesired event. In addition to these quantitative results, potential problem areas are often identified during the development of the model. These are discussed in Section 5. Table 4-1 summarizes the probability of occurrence of each of the undesired events. The number of cutsets shown in the table are those with a probability of occurrence greater than 1E-10. The overall potential for any of the events occurring which lead to the failure to perform the EDS function is 3.12E-4 (1183 cutsets), which is less than the sum of the individual events in Table 4-1. This is due to the fact that some of the cutset combinations result in failure of more than one of the functions but are correctly only counted once when looking at the overall likelihood. The listing of the first 100 cutsets (or all if less than 100 cutsets exist above 1E-10) for each of the functions is shown in Appendix C. The relative dominance of the blue pod components should not be interpreted that the blue pod is more unreliable. The model was developed for the condition with the blue pod in operation as representative. This same apparent dominance also appears in the importance measures presented in Appendix D but in fact there is no difference between the blue and yellow pods. The failure probability for the well control scenario is approximately an order of magnitude lower than for the emergency disconnect scenario.

The major contributor to the failure likelihood associated with the BOP control system results from the selected stack configuration. With only one shear ram capable of sealing the well in, it is extremely difficult to remove all the single failure points from the control system. The final shuttle valve, which supplies the hydraulics to the blind shear ram, represents such a single failure point for the disconnect function.

Table 4-1: PROBABILITY OF OCCURRENCE OF EACH OF THE UNDESIRED EVENTS

Undesired Event	Probability of Occurrence (per demand)	Number of Cutsets
Failure to perform EDS functions	3.12E-4	1183
Failure of the shear rams	2.06E-4	524
Failure to disconnect the riser from the stack	3.61E-5	753
Failure to close the upper and lower choke lines	3.32E-5	66
Failure to close the upper and lower kill lines	3.32E-7	66
Failure of well control operations	3.70E-5	612
Failure of well control using shear or pipe rams, *including choke and kill*	2.19E-5	525
Failure to close upper and lower annular	1.66E-5	313

The dominant failure combinations (in terms of probability of occurrence) associated with the failure of the BOP to perform the Emergency Disconnect Sequence when required are:

- Failure of the final shuttle valve providing hydraulic supply to the blind shear ram close port,
- Failure of a pair of choke or kill valves to close on demand,
- Failure of the indication to identify need to initiate EDS or operator failure to initiate EDS,
- Failure of the final shuttle valve providing hydraulic supply to the casing shear ram close port and the presence of casing in the stack,

589604669

- Common cause failure of all four pod modems or all four communication/power distribution panel modems

As noted above, due to the selected stack configuration, the final shuttle valve which supplies the blind shear ram represents a single failure point and accounts for 56% of the failure likelihood of the system to perform an EDS.

The failure of the four choke or kill valve pairs each contribute about 5% of the failure likelihood of the system for disconnect. This is a more significant contribution than has been found in past analyses due to their less frequent testing schedule (i.e., once a week operation of the valves rather than the daily operation of the valves for other systems.

The dominant failure combinations associated with well control operations show that the additional diversity and redundancy available for well control provide additional reliability. The likelihood of failure for the critical functions for well control is almost an order of magnitude below that for disconnect. The dominant faults are a little wider distributed than in the disconnect case but still represent a small subset of the number of failure scenarios.

- Failure of the indication to identify need to initiate well control actions or operator failure to initiate well control actions,
- Common cause failure of all four pod modems or all four communication and distribution cabinet modems,
- Inadequate precharge on the pod manifold regulator pilot and failure to switch to the inactive pod,
- Software error in the pod software or communication and distribution cabinet software, which are undetected.

Another result of the fault tree evaluation is the development of importance factors. The factors allow the analyst to focus in on the areas of risk which are important to system reliability. Two measures are typically calculated, the risk reduction measure and the risk increase measure.

For the evaluation of the BOP in terms of emergency disconnect, the most important factor to both risk increase and risk reduction is the final shuttle valve

associated with the blind shear ram. Since this area of the system is a single failure point, the importance of the shuttle valve reliability is magnified. Care should be taken to ensure the highest reliability possible from this valve. The maximum improvement in reliability possible by improvement of the shuttle valve is about a little more than a factor of 2. Conversely, if the reliability of the shuttle valve is underestimated either due to the limited data available or differences in the installed shuttle valve from the generic data sample, the reliability of the system may be severely impacted. The maximum increase in system unavailability due to an increased probability of shuttle valve failure is a factor about 3200. A specific data collection effort for the particular shuttle valve used in the Cameron system may remove some of the conservatism introduced by the use of generic data and reduce the dominance of this component. However care must be taken to ensure continued high reliability of the shuttle valve since it is extremely critical to the overall BOP disconnect operation. The final shuttle valve for the casing shear ram represents a similar potential problem, but it's importance with respect to the overall likelihood is reduced due to the smaller fraction of time that it's operability is required for a successful disconnect. Although the impact of failure of the casing shear ram is not as dominant, the same attention to its reliability should be paid as extended to the blind shear ram shuttle valve.

Beyond the blind ram shuttle valve, the next most critical factor to risk decrease for disconnect is the reliability of the choke and kill valves. The identified weekly valve exercise leads to a higher unavailability than if the valve were tested more frequently. Additional testing of the valves would lead, at most to a 5% reduction in the risk. If the valves are actually cycled more than once per week under the current operating philosophy, the contribution would in reality be lower.

Beyond these items, the largest potential item for reducing the risk (increasing the reliability) for both disconnect and well control operations is to ensure that the indication, recognition, and willingness of the operator to initiate the appropriate actions or to switch to the standby pod following failure in the active pod. The indication, recognition, and willingness of the operator to initiate the appropriate actions is also the next largest factor which can potentially increase the risk for failure to disconnect or failure of well control. Given the importance of the operator, it is essential that the indication available to him provides a clear picture

of the status and that the guidelines for initiating a disconnect or performing well control operations are clear and concise.

The only other factor which can potentially raise the risk by a large amount are the postulated common cause failures in the modems, power supplies, and CPU boards. These types of failures are difficult to reduce because they are generally driven by common maintenance errors, common environmental effects, common manufacturing defects, or other similar factors. In general practice, the method used to reduce the potential for common cause failures is to provide diversity, e.g., use of multiple brands of modems, power supplies, and CPU boards. This is not always practical nor desirable from a standardization point of view. Given the low risk reduction potential for these items, care should be taken to ensure that the equipment is qualified for its operational environment, and care is taken in any maintenance activities to reduce the potential for common errors in an attempt to minimize the potential for a higher common cause contribution.

The complete importance analysis results are contained in Appendix D.

5. OBSERVATIONS

Several observations were made during the course of the analysis which have an impact on the current and future reliability of the Cameron BOP control system. Overall, the system has been well designed with a large amount of redundancy in most areas. One item was identified during the model development which has already resulted in a design change in the system. A condition was identified in the system, as initially configured, in which the standby pod would be unable to be hydraulically activated upon loss of the other pod's hydraulics. The pilot operated check valve which controls the pod hot line supply would close upon loss of one pod's hydraulics. As a consequence, the standby pod would be unable to assume control since there would be no pilot supply to allow the pilot valve to be opened. The initial thought had been to keep both hot line supply open signals active. However, due to concerns over binding of the shuttle valve in an indeterminate position, the supply from the inactive pod was interlocked to be inactive via software controls. This would have resulted in closure of the pilot operated check valve upon loss of hydraulics and no ability to open the alternate pod supply except through use of an ROV. The shuttle valve supplying the pilot operated check valve was replaced with a different shuttle valve that was designed to operate with hydraulic pressure with either or both hydraulic inputs pressurized. Failure of the pod hydraulic supply under this case would result in the pilot operated check valve remaining open, since the pilot supply from the inactive pod would be available immediately upon loss of the active pod hydraulics.

The design of the system with two trains of redundant electronics in each pod allows for the potential to continue operating in a safe manner even in the event of a card failure or modem failure. Although some increased risk must be expected if operation continues with a failure in the pod, this increased risk must be examined with respect to the time remaining in the drilling operation. Since the risk increase due to the failure of a single train of pod electronics is extremely minor ($< 1\%$) even if exposed for the entire duration of the drilling operation this will not likely be the governing concern. This is due to the dominance of hardware faults in the hydraulic portions of the system. If a second train of electronics fails, but in a different pod, the risk is increased as would be expected. The increase however is not extremely significant ($< 5\%$), again due to the dominance of non-electronic faults. If the

second train of electronics is within the same pod, i.e., complete loss of pod functionality, the risk is significantly increased (970% - from 3.1E-4 to 3.3E-3) if drilling operation continues under these circumstances.

Several areas were identified during the course of the analysis which tend to drive the reliability results. The most significant is the use of a single blind shear ram in the specified stack configuration. This is a condition imposed upon the control system due to the selected stack configuration. Control system design alterations to improve the configuration's reliability would not be practical. Therefore, it is more important to be cognizant of the potential vulnerability, to strive to use the most reliable robust shuttle valve available, and to be aware of its importance during the installation and any maintenance activities involving the valve.

As indicated in the discussion of dominant contributors, the weekly demonstrations of operability for the choke and kill valves influence their reliability. More frequent operability testing can reduce the failure likelihood. However, potential impacts to the normal drilling operation arising from such changes to testing frequency must be also taken into consideration.

The arrangement of the solenoid cables/connectors on the pod piggyback/carrier boards has an effect on the system reliability. Each train of subsea pod electronics contains fourteen piggyback boards and seven carrier boards. Cameron has ensured that the circuits are assigned such that redundant functions do not utilize the same carrier board or piggyback board. If an entire board were to fail, the full complement of redundant features would be maintained. Due to the overall redundancy designed into the system, this does not significantly impact the overall system reliability, however it does reflect good reliability engineering practice.

One potential conservatism included in previous analyses of the system, which has been removed for this analysis, is the inclusion of the requirement for the annular to open in order for EDS to be successful. Although desirable, opening of the annular is not considered to be essential to successful EDS.