DYNAMIC POSITIONING CONFERENCE

October 12-13, 2010

RELIABILITY SESSION

FMEA Failed to Meet Expectations Again (Again?)

By (Doug Phillips, Brian Haycock, Steven Cargill)

(DP Expertise, BHDP Services, GL Noble Denton)

Return to Session Directory

Abstract

- 2001 – Fail to Meet Expectations Again
- Many FMEA's improved since
- Improvements led by .....
- 100 or more FMEA's reviewed
- Still problematic to produce
- Many single point failures overlooked

Introduction

Part 1

- Impediments to the FMEA process

Part 2

- Commonly overlooked failure modes

Part 1- FMEA

A Failure Modes and Effects Analysis (FMEA) of the DP System is a classification society requirement for DP Class 2 and DP Class 3 vessels

Key Responsibilities

- Define WCFDI/post failure DP capability
- Designers consider WCFDI
- Shipyard must understand WCFDI
- Competent FMEA and proving Trials
- Class to confirm design of DP and standard of FMEA

Complexity of Modern Vessels

- Diesel Electric power plants
- PLC's, Microcontrollers
- Data networks
- Layers of control
- Bespoke protective functions

Redundancy versus Fault Tolerance

Design Verification

- FMEA requested
- Design verification expected

Dealing With Complexity

Multidisciplinary engineering team

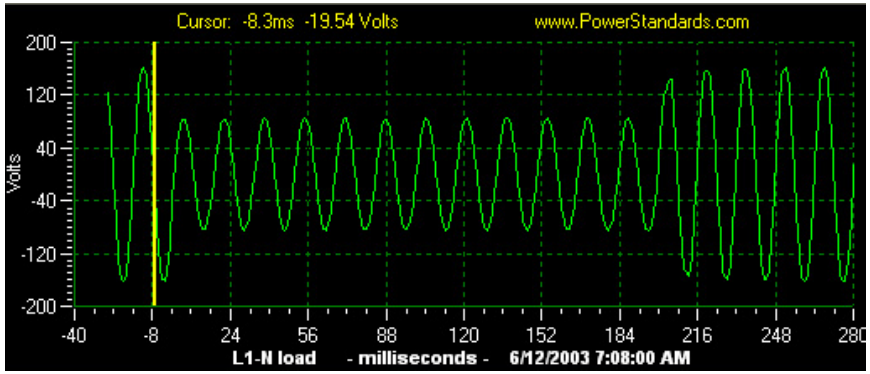
- Marine Engineer
- Electrical Engineer
- Control Systems Engineer

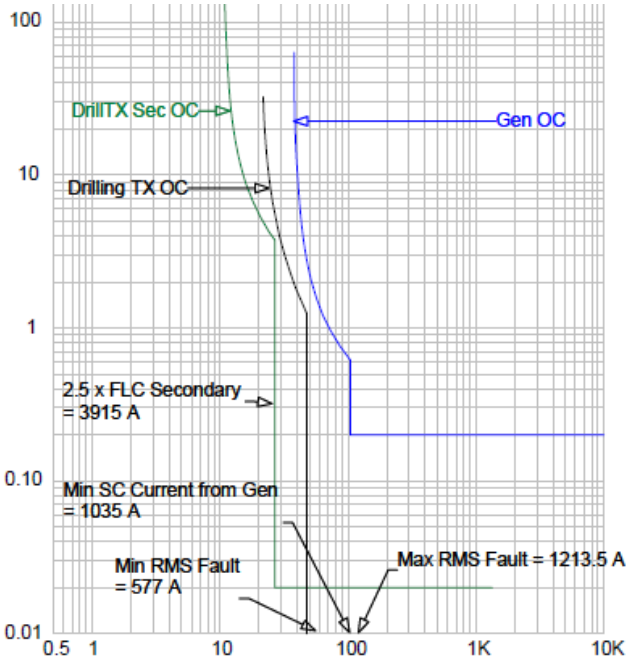
Operating configurations clearly defined

- Common bus
- Two or more independent power systems
- Multiple configurations

Supporting Studies

- Protection Co-ordination
- Power plant stability
- Harmonics
- Voltage dip





Commercial Pressures

Cost =

- Complexity of vessel & depth of FMEA

Varying Standards:-

- If Class/owners accept less detailed FMEAs

Lack of Detailed Information

- Pressure to deliver preliminary FMEA
- Raises more questions than it answers

Better approach:-

- Redundancy concept document
- Use drawing review process

Limitations on Testing

- Wire breaks, shut down, erroneous signals
- HIL?

Sea trials, pressure to reduce testing time

Best results:-

- FMEA proving after all commissioning complete

Reliability of Information

- How to verify/prove complex design?
- Proof by testing preferred
- Not always comprehensive

Ideal for proving protection/volt dip:-

- Apply a real short!
- Now required by at least one major class

Competence of FMEA Provider

- Shortage of highly experienced personnel
- Consultancies ‘home growing’
- New personnel adequately supervised
- Adequate QA of final product

Key Elements of Analysis

- Failure modes and effect
- Hidden Failures
- Common Mode failures
- Configuration errors
- Acts of Maloperation

FMEA Formats

- Narrative form vulnerable to omissions
- Tabular form restrictive on space
- Use structured template with headings:-

Within each subsystem there are the following headings. – Replace the word ‘system’ with appropriate name e.g. ENGINES AND AUXILIARY SYSTEMS. Replace ‘subsystem’ with the appropriate name e.g. FUEL OIL SYSTEM.

SYSTEM

SUBSYSTEM

1. Document reference
2. Description, and redundancy concept – (including simplified sketch of subsystem)
3. Location
4. Configuration for DP
5. Failure modes of the subsystem
6. Effects of subsystem failures
7. Hidden subsystem failures
8. Common mode failures
9. Configuration errors
10. Acts of maloperation
11. Worst case failure of the subsystem

FMEA Management Tools

- Technical query form
- Technical query register
- Assumptions register
- Maintenance and testing issues register
- Concerns register
- Progress reports
- Conclusions & recommendations

Part 2 – Introduction

- Many FMEA's improved since
- 100 or more FMEA's reviewed
- Many single point failures overlooked
- Operational constraints

Safest Mode of Operation

- Duty/standby pumps
- Independent fuel oil/cooling systems etc
- Operation of changeovers
- UPS batteries
- DP control set up
- Selection of PRS and sensors

Safest Mode of Operation

Open bus tie because we can't satisfy ourselves that:-

- AVR failure
- Governor failure
- Bus tie hidden failure
- Protection configuration error
- Under voltage, etc.

Won't cause a blackout or loss of thrusters

Full load capacity and load acceptance

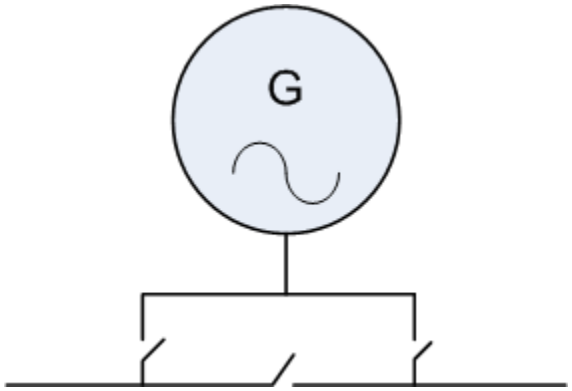
- Diesels/thrusters tested at 100%
- Load acceptance from <50% to 100%
- Operate below approx 50%(two thrusters)
- 33% three thrusters – two with common failure mode
- Consider lever arms/ratings

Deficiencies in Consequence Analysis

- Only considers WCF
- Assumes protection will operate
- Fuel Oil, DP I/O layout not covered

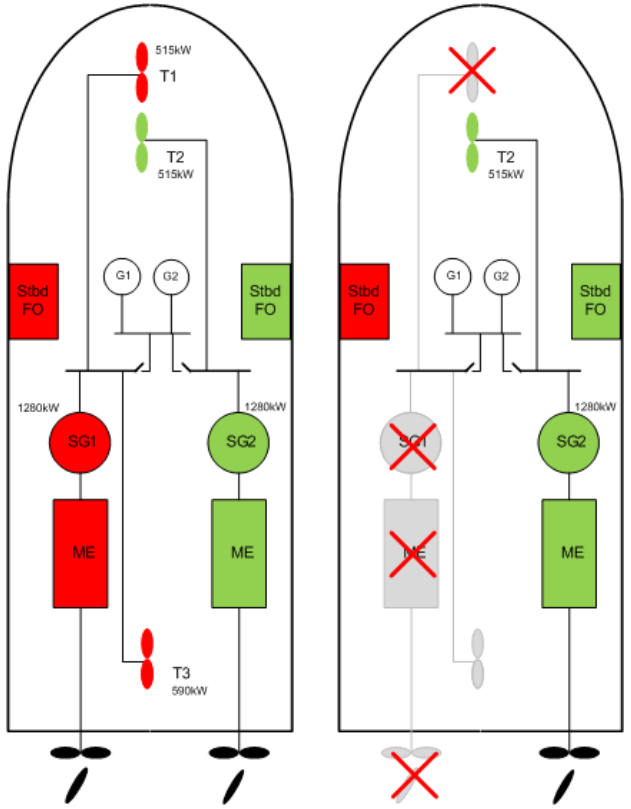
Assignable Generators and Thrusters

- DP I/O allocated to single module
- SW/FW Cooling changeover?
- Fail modes depend on assignment



Inclusion of Props and Rudders

- Single stern thruster
- Rudders only effective with prop ahead
- Failed ME leaves one prop/one rudder
- Environment dependant



Specific DP Applications

Heavy Lift crane Barge

- Heavy lift mode

Shuttle Tanker

- Fishtailing/Surging

Failure of External Force Signal

- Pipe layer/ Shuttle tanker etc
- Feed forward term
- Failure of signal could cause drive off
- FMEA should check failure mode of signals

Suitability of PRS for Application

MSC645:-

- At least three
- >2 different principles

- Deepwater drillships and OSV's
- Relative PRS at spars

Independence of PRS

- Power supplies (UPS)
- I/O to DP
- Input of sensors
- Changeover switches

Backup DP Supplies

- 24Vdc + 230V/24Vdc PSU
- Blocking diodes
- Comprehensive monitoring?
- Fail to high voltage
- Overvoltage protection?

Common Mode Engine Failures

- Closure of all engine room fire dampers
- Spurious operation of crankcase pressure sensors
- Oil mist detectors

Location of DP Sensors

MRUs

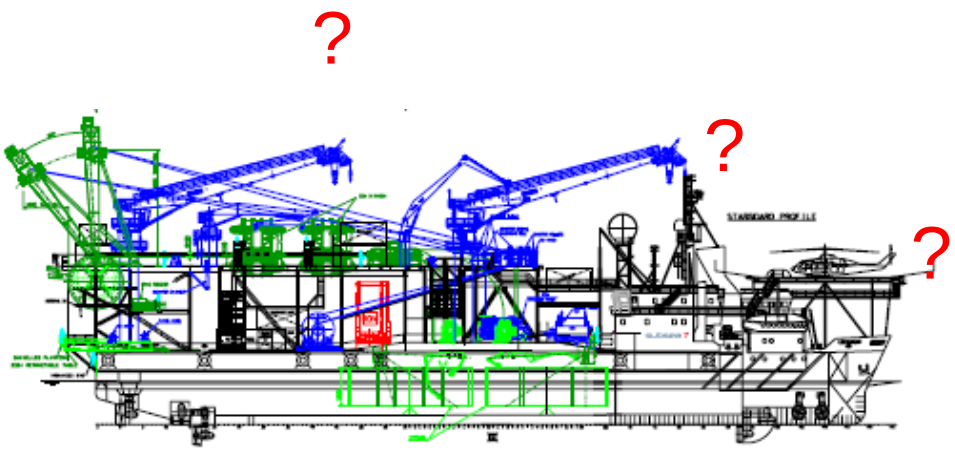
- Close to C of G?

Wind sensors

- Clear of obstructions causing turbulence/blocking
- Only one blocked at a time

Gyros

- If only 2 – magnetic near DP console?



Operational Errors

"Should be considered if reasonably foreseeable"

Examples

- E.stop wrong thruster/engine
- Operator pressed 'present position' when DP was recovering from excursion

Systemic Failures

DPC system – separate S/W and H/W?

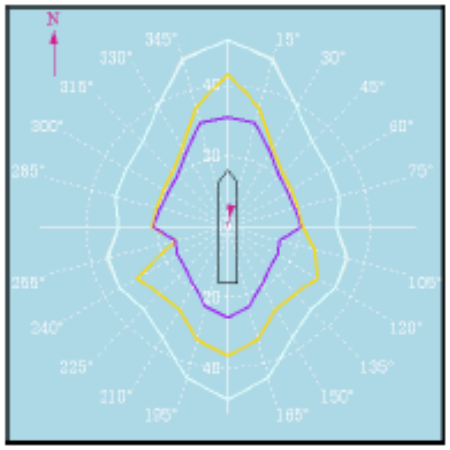
- Rigorous testing
- HIL

Consider providing diversity of sensors

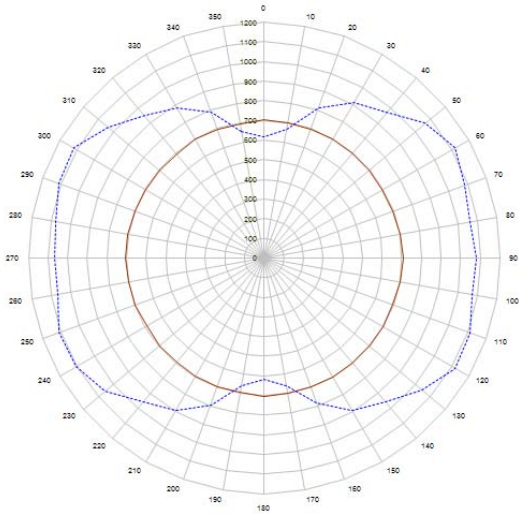
Capability Plots Not Considering WCF

ERN - Intact case / Least effective thruster / Most effective thruster

Verification

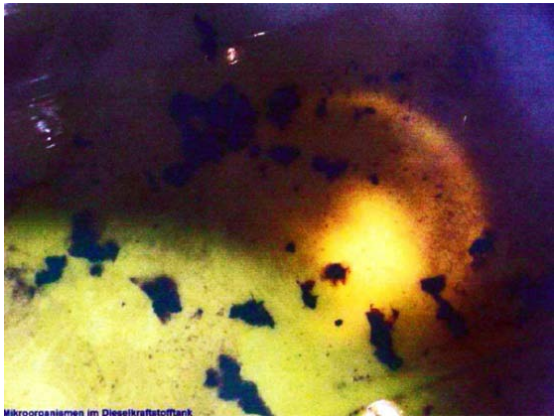


Different formats



Fuel Contamination

- Pipe fractures
- Water contamination
- Microbiotic contamination
- Use of high/low suction
- Purifier gravity discs/throughput
- Staggered fuel from bunkers



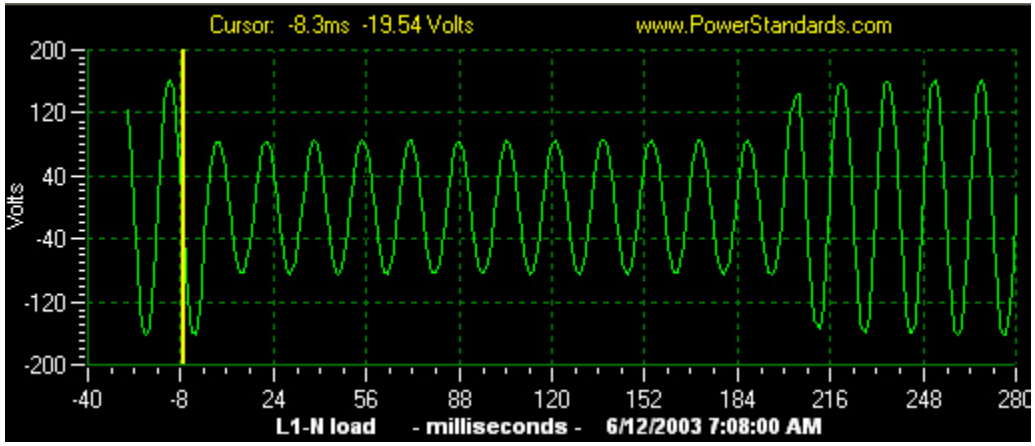
Risk of Engine Room Fires

Can engines be isolated in line with redundancy concept?

- Preventative measures in place?:-
- Double skinned high pressure piping
- Fuel leak detection
- No hotspots

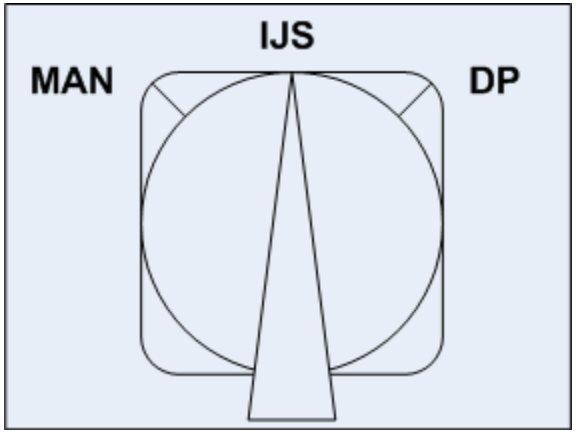
Undervoltage Trips

- Severe voltage dips
- Source of common mode failure
- Especially closed bus
- Generators, drives, transformers, pumps fans



DP/Manual/IJS Changeover

- Often single multiwafer switch
- Better - Individual switch per thruster
- Avoid common power supply
- Network / software changeover



Conclusions

- Multidisciplinary teams/Supporting studies
- Appeal to Class/Owners to demand minimum standard of FMEA
- Use template to avoid missing important failure modes & tracking tools to monitor process

- Many single mode failures still overlooked
- Barriers in Safest Mode of Operation
- Activity and suitable modes not considered
- Suitable position references not considered

DYNAMIC POSITIONING CONFERENCE

October 12-13, 2010

RELIABILITY SESSION

FMEA Failed to Meet Expectations Again (Again?)

By (Doug Phillips, Brian Haycock, Steven Cargill)

(DP Expertise, BHDP Services, GL Noble Denton)