

# MSC Guidelines for Review of Qualitative Failure Analysis

**Procedure Number: E2-18**

**Revision Date: 04/28/00**

---

## References

- a. Title 46 CFR Parts 58, 61 and 62
  - b. Title 46 CFR Parts 111 and 112
  - c. Navigation and Inspection Circular (NVIC) 2-89, "Guide for Electrical Installations on Merchant Vessels and Mobile Offshore Drilling Units"
  - d. American Bureau of Shipping (ABS), "Rules for Building and Classing Vessels under 90 Meters in Length", 1996
  - e. Safety Of Life at Sea (SOLAS), Consolidated Editions, 1997, Chapter II-1, Part D
  - f. MSC Procedure E2-1, Vital System Automation Work Instruction
- 

## Disclaimer

These guidelines were developed by the Marine Safety Center staff as an aid in the preparation and review of vessel plans and submissions. They were developed to supplement existing guidance. They are not intended to substitute or replace laws, regulations, or other official Coast Guard policy documents. The responsibility to demonstrate compliance with all applicable laws and regulations still rests with the plan submitter. The Coast Guard and the U. S. Department of Transportation expressly disclaim liability resulting from the use of this document.

---

## Contact Information

If you have any questions or comments concerning this document, please contact the Marine Safety Center by e-mail or phone. Please refer to the Procedure Number: **E2-18**

E-mail: [customerservicemsc@msc.uscg.mil](mailto:customerservicemsc@msc.uscg.mil)

Phone: 202-366-6480.

---

## General Review Guidance

- QFA General Acceptance Criteria:
    - a. Failsafe state must be evaluated for each subsystem, system or vessel to determine the least critical consequence. Lowest level of system component failure to be considered is: "easily replaceable component." 46 CFR 62.30-1(a).
    - b. All automatic control, remote control, safety control, and alarm systems must be failsafe. See 46 CFR 62.30-1(b).
-

# MSC Guidelines for Review of Qualitative Failure Analysis

**Procedure Number: E2-18**

**Revision Date: 04/28/00**

---

- c. Single non-concurrent failures in control, alarm, or instrumentation systems, and their logical consequences, must not prevent sustained or restored operation of any vital system or systems. See 46 CFR 62.30-5(a).
- d. For typical failsafe states, see 46 CFR Table 62.10-1(a)
- e. Failure of an automatic control, remote control, or alarm system must be immediately alarmed in the machinery spaces and at the ECC (if provided). 46 CFR 62.25-20(d)(6).
- f. When the machinery plant is unattended, failure alarms of vital systems requiring the immediate attention of the bridge watch officer for the safe navigation of the vessel must be extended to the bridge. Extension of these alarms to the engineers' accommodations is also required. 46 CFR 62.50-30(f).
- g. For each vital system or systems, normal source of supply should be included in the QFA. See 46 CFR 62.30-5(c).
- Identification of "easily replaceable components" to be included in the QFA. Using the system's internal component layout plan submittal, identify "easily replaceable components". Relays, terminal boards, indicator lights, switches, wire harness, meters or instruments, and relay contacts need not be considered. The focus should be on electronic circuit boards, circuit power supplies, processors, memory boards, input/output modules, microcontrollers, communication boards, circuit drivers, and similar circuit boards containing solid state devices. Each "easily replaceable component" identified above should be included in the QFA.
- What to look for in the QFA document. For each failure considered, check the following items:
  - a. Acceptable Failure Effects (failsafe)
  - b. Failure Detection (audible and visual alarms) by the crew in appropriate locations, (e.g. navigating bridge, ECC, machinery spaces, and engineers' accommodations, as required)
  - c. Alternatives or Control Alternatives available to the crew.

# MSC Guidelines for Review of Qualitative Failure Analysis

**Procedure Number: E2-18**

**Revision Date: 04/28/00**

---

- Operating Assumptions: The QFA must be prepared assuming the vessel is in its normal condition of operation and reflect the level of automation and manning level of the machinery plant, e.g., vessel underway in pilothouse control, all main engines in remote automatic operation, machinery space manned or unattended (depending on the vessel's manning level), and automatic power management system, if provided, is active.

## Failure Effects

- Checking the QFA's Failure Effects:
  - a. Propulsion Control Systems. 46 CFR 62.35-5(e)(3).
    - (1) Failures of the remote propulsion control system should be failsafe, such that the preset speed and direction (as-is) of thrust is maintained, until local manual or alternate manual control is in operation, or the manual safety trip (shutdown) is activated. This is required specifically for vessels with a single propulsion plant or single propeller.
    - (2) For a vessel with multiple and independently controlled propellers, a failure of one propulsion control system need not follow the failsafe requirements above. The failsafe options available in this case are:
      - (i) Force both control systems to fail "as-is." Systems respond like a vessel with a single propulsion plant.
      - (ii) Fail "as-is" of just the affected control system, while maintaining full control of the unaffected propulsion system.
      - (iii) Fail to "zero" thrust or trip of the affected propulsion system, providing partial reduction of normal propulsion capability as a result of malfunction or failure. Reduced capability should not be below that necessary for the vessel to run ahead at 7 knots or half-speed of the vessel, whichever is less, and is adequate to maintain control of the ship. This adopts the intent of the "Note" in 46 CFR 58.01-35.

# MSC Guidelines for Review of Qualitative Failure Analysis

**Procedure Number: E2-18**

**Revision Date: 04/28/00**

(3) Independent Sensors: The failure analysis must demonstrate that sensors for primary speed, pitch or direction of rotation control in a closed loop propulsion control system are independent and physically separate from required safety control, alarm, or instrumentation sensors. 46 CFR 62.30-5(b)(2).

b. Safety Control Systems.

(1) Failure of the normal electrical power source to this system must not cause a shutdown, unless it is determined to be the failsafe state. 46 CFR 62.25-15(b).

(2) Propulsion control loop sensors must not be used as sensors to provide safety trip control. 46 CFR 62.30-5(b)(2).

(3) The propulsion manual safety trip (emergency shutdown) must be independent and physically separate from all other systems. This is necessary when the failsafe state of the propulsion control system maintains the preset speed and direction (as-is) of thrust, to provide an independent system to stop the propulsion system if necessary. 46 CFR 62.30-5(b)(3).

c. Automatic Power Management. For the least critical consequence for this system, failures must not cause a dead-ship condition.

d. Monitoring and Alarm System. Propulsion control loop sensors must not be used as alarm sensors. 46 CFR 62.30-5(b)(2).

## Failure Detection

- Checking the QFA's Failure Detection: Failure alarms must be audibly and/or visually annunciated at required locations. The manning level of the machinery plant must be given consideration. See the QFA's general acceptance criteria above.
- Checking the QFA's Alternatives or Control Alternatives.

## Alternatives or Control Alternatives

a. Propulsion Control Systems.

(1) Local manual or alternate manual control must be available. 46 CFR 62.25-10(a)(1) and 62.35-5(e)(3).

# MSC Guidelines for Review of Qualitative Failure Analysis

**Procedure Number: E2-18**

**Revision Date: 04/28/00**

---

- (2) Manual alternate control systems must include means to override automatic controls and interlocks, as applicable. 46 CFR 62.25-10(a)(2).
- b. Safety Control Systems. Local manual safety trip controls must be provided for all turbines and internal combustion engines.
- c. Automatic Power Management. Local manual generator and switchboard instrumentation and controls, as applicable in 46 CFR 111.12-11 and 111.30-24, -25, and -27, must remain functional.
- d. Monitoring and Alarm System.
  - (1) Manual control locations, including remote manual control, and manual alternate control, must be provided with the instrumentation necessary for safe operation from that location. 46 CFR 62.25-20(b)(1).
  - (2) Systems with remote instrumentation must have provisions for the installation of instrumentation at the monitored system equipment. 46 CFR 62.25-20(b)(2).

---

Attachments

None