U.S. COAST GUARD MARINE SAFETY CENTER PLAN REVIEW GUIDELINE

REVIEW OF QUALITATIVE FAILURE ANALYSIS

Procedure Number: E2-18
Revision Date: October 27, 2021

S. M. Peterson CDR, Chief, Engineering Division

Purpose

This Plan Review Guideline (PRG) explains the requirements for plan submittal for Qualitative Failure Analysis (QFA) in accordance with the references below. This PRG should be used as a guide for an automated vital system.

Contact Information

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

E-mail: msc@uscg.mil
Phone: 202-795-6729
Website: www.dco.uscg.mil/msc

Table of Contents

1. Applicability

This Plan Review Guideline (PRG) is applicable to self-propelled vessels that are 500 gross tons and over and certificated under subchapters D, I, or U, to self-propelled vessels that are 100 gross tons and over and are certificated under subchapter H, and to OSVs of at least 6,000 GT ITC (500 GRT if GT ITC is not assigned) as defined in 125.160 of this chapter.

2. References

Title 46 CFR Parts 58, 61 and 62
Title 46 CFR Subchapter J, Electrical Engineering
Navigation and Inspection Circular (NVIC) 2-89, "Guide for Electrical Installations on Merchant Vessels and Mobile Offshore Drilling Units"
Safety of Life at Sea (SOLAS), Consolidated Edition, 2014: Chapter II-1, Part D
MSC Plan Review Guideline, E2-01, Review of Vital System Automation
MSC Plan Review Guideline, E2-05, Design Verification Test Procedures
MSC Plan Review Guideline, E2-17, Periodic Safety Test Procedures
CG-ENG-Policy Letter No. 02-19 "Design Guidance for Lithium-Ion Battery Installations Onboard Commercial Vessels"

3. Definitions

Easily replaceable component-using the submitted system internal component layout plan and the bill of materials, easily replaceable components are items that can be replaced. This does not include any components such as relays, terminal boards, indicator lights, switches, wire harness, meters, instruments, and relay contacts. 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. Using the applicable QFA procedures in the 46 CFR 62.20-3 (Note), the above easily replaceable components would be evaluated to:

a. An acceptable failsafe state per 46 CFR 62.30-1
b. Failure detection (audible and visual alarms) by the crew in the appropriate locations. IE: navigating bridge, ECC, machinery spaces and engineers' accommodations, as required.
c. Local control or other alternatives available to the crew

4. Content

General Acceptance Criteria

a. A qualitative Failure Modes Effects Analysis (FMEA) may be considered as an acceptable QFA.

b. The QFA should indicate automation assumptions, vessel/equipment operating conditions, failures considered, cause and effect relationships, method of crew detection of failure and alternatives available to the crew. Please see 46 CFR 62.20-3(Note).

c. As required by 46 CFR 62.20-3(b), and as applicable to the particular automated vital system submitted for the vessel, the QFA must contain:

(1) Propulsion controls.
(2) Microprocessor based system hardware.
(3) Safety controls.
(4) Automated electric power management.
(5) Automation required to be independent that is not physically separate.
(6) Other automation that potentially constitutes a safety hazard to crew or vessel if failed, as judged by the Coast Guard.

d. A failsafe state as defined in 46 CFR 62.10-1 must be evaluated for each subsystem, system or vessel to determine the least critical consequence. The lowest level of system component failure is identified as an "easily replaceable component". All automatic control, remote control, safety control, and alarm systems must be failsafe as required by 46 CFR 62.30-1(a)(b).

e. 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 in compliance with 46 CFR 62.30-5(a).

f. For typical failsafe states, refer to 46 CFR Table 62.10-1(a).

g. Failure of an automatic control, remote control or alarm system must immediately alarm the machinery spaces and Engineering Control Center (ECC) (if provided). Please see 46 CFR 62.25-20(d)(6).

h. Operating programs for microprocessor based or computer based vital control, alarm and monitoring systems must be stored in non-volatile memory and automatically operate on resumption of supply power as required by 46 CFR 62.25-25(b).

i. Automatic propulsion systems, automated electric power management systems and all associated subsystems and equipment must be capable of meeting load demands from standby to full system rated load, under steady state and maneuvering conditions without need for manual adjustment or manipulation in compliance with 46 CFR 62.35-1(b).

j. When the machinery plant is periodically unattended, ECC alarms for vital systems that require 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).

k. The QFA must be prepared assuming the vessel is in a normal operating condition and it reflects a level of automation and manning of the machinery plant. For example, the vessel is underway under pilothouse control, all main engines set in remote automatic operation, the machinery space is manned or is unattended (depending on vessel manning level), and the automatic power management system is active (if installed).

Failure Effects of the QFA

a. Remote propulsion control system (PCS) failsafe state is required to be as-is per Table 46 CFR 62.10-1(a) and 62.35-5(e)(3). As-is condition maintains the preset (as is prior to failure)

speed and direction of thrust until local or alternate manual control is in operation, or the manual safety trip (emergency stop) control is activated. Failure of any remote PCS component, including the loss of the PCS speed, direction, or pitch output command signal to the propulsion system must not have any effect on main propulsion. To demonstrate the as-is failsafe state, DVTP testing should including failure of the PCS controller and PCS output speed, direction, and pitch command (CPP) output signals. Failure of the PCS controller may be simulated by securing all power sources to the PCS controller.

b. When the evaluation of the automated vital system failsafe state required per 46 CFR 62.30-1(a) determines a failsafe state that conflicts with the failsafe state shown in Table 46 CFR 62.10-1(a), the failsafe state must be submitted under equivalents. Demonstration of functional equivalence must include comparison of a QFA based on the requirements of 46 CFR Part 62 with a comparable analysis of the proposed failsafe state, see 46 CFR 62.15-1(a).

c. The QFA must demonstrate that independent 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).

d. Safety trip controls must not operate as a result of failure of the normal electrical power source to this system, unless the trip control is determined to be the failsafe state 46 CFR 62.25-15(b).

e. Propulsion control loop and propulsion manual safety trip (emergency shutdown) sensors must be independent and physically separate from required safety trip controls as per 46 CFR 62.30-5(b)(2) or from all other systems as per 46 CFR 62.30-5(b)(3). This is necessary at a failsafe state of the propulsion control system in order to maintain preset (as is) speed and direction of thrust, and provide an independent system to stop the propulsion system if necessary.

f. In a least critical consequence for automatic power management, a failure in the system must not cause a dead-ship condition.

g. In monitoring and alarm systems, propulsion control loop sensors must not be used as alarm sensors 46 CFR 62.30-5(b)(2).

Alarms and Alternative Controls

a. Failure alarms must be audibly and/or visually annunciated at required locations. Manning level of the machinery plant may impact alarm locations. See 46 CFR 62.25-20(d).

b. Manual alternate control systems must be operable in an emergency and after remote or automatic primary control system failure. A remote propulsion control system must be failsafe and maintain preset (as is) speed and direction of thrust until local manual or alternate manual control occurs, or operation of a manual safety trip control. As applicable, manual alternate control systems must include means to override automatic controls and interlocks. See 46 CFR 62.25-10(a)(1)(2) and 46 CFR 62.35-5(e)(3).

(1) Safety trip controls are required for specific automated vital systems. See 46 CFR Table 62.35-50.

(2) Manual control locations, including remote manual control and manual alternate control, must be provided with instrumentation necessary for safe operation from that location. Systems with remote instrumentation must have provision for installation of instrumentation at the monitored system equipment. See 46 CFR 62.25-20(b)(1)(2).

Lithium-ion Battery Installations

a. As outlined in the CG-ENG Policy Letter No. 02-19, all lithium-ion battery installations must submit a QFA that analyzes the effects of individual component failure on the safety and reliability of the power system. This is done by identifying each easily replaceable component from the bill of materials and confirming that single non-concurrent failures in the control, alarm, or instrumentation systems will not prevent sustained or restored operation.

b. Failure of the overall system, if individual components are contained in that system, does not provide the analysis to demonstrate the failure of an easily replaceable component. This analysis is critical to identifying what the expected failure outcome, alarms, and alternative methods or controls are available to the crew, and will not produce unexpected results.

c. The QFA should include interconnections between propulsion control, power management, and the battery management system.

d. Any sensors that cannot be easily replaced should still be included in the analysis, but when testing in the DVTP, should provide an explanation as to why the sensor cannot be tested. For example, a temperature sensor embedded in the battery cell that cannot be removed, should be included in QFA to provide what the expected failure of that sensor and the crew's notification of that failure.

5. Disclaimer

This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally-binding requirements on any party. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the general public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative, you may contact MSC, the unit responsible for implementing this guidance.