MSC Guidelines for Qualitative Failure Analysis

Procedure Number: E2-18 Revision Date: 11/10/2011

S. J. Kelly , CDR, Chief, Engineering Division

Purpose:

To establish MSC Plan Review Guidelines for a Qualitative Failure Analysis (QFA) for a vessel automated vital systems.

References:

a. Title 46 CFR Parts 58, 61 and 62

b. Title 46 CFR Subchapter J, Electrical Engineering

c. Navigation and Inspection Circular (NVIC) 2-89, "Guide for Electrical Installations on Merchant Vessels and Mobile Offshore Drilling Units," can be found at: http://www.uscg.mil/hq/cg5/nvic/pdf/1989/n2-89.pdf

d. Safety Of Life at Sea (SOLAS), Consolidated Edition, 2009: Chapter II-1, Part D

e. MSC Plan Review Guideline, E2-01, Review of Vital System Automation

f. MSC Plan Review Guideline, E2-17, Periodic Safety Test Procedures

g. MSC Plan Review Guideline, E2-05, Design Verification Test Procedures

Contact Information:

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

Email: MSC@uscg.mil
Phone: 202-475-3402
Website: http://homeport.uscg.mil/msc

Responsibilities:

Using applicable portions of references (a) through (g), the submitter shall provide sufficient documentation and plans to indicate compliance with the applicable requirements. To facilitate plan review and project management, all plans and information specified in these guidelines should be submitted as one complete package through a single point of contact for the project. The submission shall be made in triplicate if a stamped copy is desired.

General Guidance:

- The QFA is applicable to self-propelled vessels that are 500 gross tons and over and certificated under subchapters D, I, or U, and to self-propelled vessels that are 100 gross tons and over and are certificated under subchapter H. Please refer to 46 CFR 62.01-5(a).

- A qualitative Failure Effects Modes Analysis may be considered as an acceptable QFA.

- QFA General Acceptance Criteria:

  a) 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).

  b) As per 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.

  c) A failsafe (46 CFR 62.10-1) state 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 (46 CFR 62.30-1(a)(b)).

  d) 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 (46 CFR 62.30-5(a)).

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

f) 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).

g) 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 (46 CFR 62.25-25(b)).

General Guidance (continued):

h) 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 (46 CFR 62.35-1(b)).

i) 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)).

- Identification of an "*easily replaceable component*" that would be included in the QFA:

  a) Using the submitted system internal component layout plan, identify easily replaceable components. Relays, terminal boards, indicator lights, switches, wire harness, meters, instruments and relay contacts need not be considered. 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:

     1. An acceptable Failure Effects (failsafe).

     2. Failure detection (audible and visual alarms) by the crew in the appropriate locations. IE: navigating bridge, ECC, machinery spaces and engineers' accommodations, as required.

     3. Control or other alternatives available to the crew.

- Operating Assumptions:

    a) 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).

General Guidance (continued):

- A Check of the Failure Effects of the QFA:

    a) The remote propulsion control system must be failsafe by maintaining the preset (as is prior to failure) speed and direction of thrust maintained, until local or alternate manual control is in operation, or the manual safety trip (shutdown) control is activated.
    This is required for vessels with a single propulsion plant or single propeller (46 CFR 62.35-5(e)(3)).

    b) For a vessel with multiple and independently controlled props, a failure of one propulsion control system need not follow above failsafe requirement. In this case, failsafe options available:

        1. Force both prop control systems to fail "as is." Systems should respond in a similar fashion to a vessel with a single propulsion plant.

        2. Fail to "as is" for only the affected control system, while maintaining full control of the unaffected propulsion system.

        3. Fail to "zero" thrust or trip off the affected propulsion system, thus resulting in partial reduction of normal propulsion capability due to the malfunction or failure. Reduced speed should not be below that necessary for the vessel to run ahead at 7 knots or at half speed of the vessel, whichever is less, and is adequate to maintain control of the ship (46 CFR 58.01-35 (Note)).

    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)).

General Guidance (continued):

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)).

- 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).

- 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).

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

  b) 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).

Attachments None

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 the Marine Safety Center (MSC), the unit responsible for implementing this guidance.