## TASK 208
## FUNCTIONAL HAZARD ANALYSIS

208.1 Purpose. Task 208 is to perform and document a Functional Hazard Analysis (FHA) of an individual system or subsystem(s). The FHA is primarily used to identify and classify the system functions and the safety consequences of functional failure or malfunction, i.e. hazards. These consequences will be classified in terms of severity for the purpose of identifying the safety-critical functions (SCFs), safety-critical item (SCIs), safety-related functions (SRFs), and safety-related items (SRIs) of the system. SCFs, SCIs, SRFs, and SRIs will be allocated or mapped to the system design architecture in terms of hardware, software, and human interfaces to the system. The FHA is also used to identify environmental and health related consequences of functional failure or malfunction. The initial FHA should be accomplished as early as possible in the Systems Engineering (SE) process to enable the engineer to quickly account for the physical and functional elements of the system for hazard analysis purposes; identify and document SCFs, SCIs, SRFs, and SRIs; allocate and partition SCFs and SRFs in the software design architecture; and identify requirements and constraints to the design team.

208.2 Task description. The contractor shall perform and document a FHA to analyze functions associated with the proposed design. The FHA should be based on the best available data, including mishap data (if obtainable) from similar systems and other lessons learned. This effort will include inputs, outputs, critical interfaces, and the consequence of functional failure.

208.2.1 At a minimum, the FHA shall consider the following to identify and evaluate functions within a system:

a. Decomposition of the system and its related subsystems to the major component level.

b. A functional description of each subsystem and component identified.

c. A functional description of interfaces between subsystems and components. Interfaces should be assessed in terms of connectivity and functional inputs and outputs.

d. Hazards associated with loss of function, degraded function or malfunction, or functioning out of time or out of sequence for the subsystems, components, and interfaces. The list of hazards should consider the next effect in a possible mishap sequence and the final mishap outcome.

e. An assessment of the risk associated with each identified failure of a function, subsystem, or component. Estimate severity, probability, and Risk Assessment Code (RAC) using the process described in Section 4 of this Standard. The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with Department of Defense (DoD) Component policy.

f. An assessment of whether the functions identified are to be implemented in the design hardware, software, or human control interfaces. This assessment should map the functions to

their implementing hardware or software components. Functions allocated to software should be mapped to the lowest level of technical design or configuration item prior to coding (e.g., implementing modules or use cases).

g. An assessment of Software Control Category (SCC) for each Safety-significant Software Function (SSSF). Assign a Software Criticality Index (SwCI) for each SSSF mapped to the software design architecture.

h. A list of requirements and constraints (to be included in the specifications) that, when successfully implemented, will eliminate the hazard or reduce the risk. These requirements could be in the form of fault tolerance, detection, isolation, annunciation, or recovery.

208.2.2 The contractor shall update the FHA following system design or operational changes as necessary.

208.2.3 The contractor shall document results of the analysis to include the following:

a. System description. This summary describes the physical and functional characteristics of the system and its subsystems. Reference to more detailed system and subsystem descriptions, including specifications and detailed review documentation, shall be supplied when such documentation is available.

b. Hazard analysis methods and techniques. Provide a description of each method and technique used in conduct of the analysis. Include a description of assumptions made for each analysis and the qualitative or quantitative data used.

c. Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used. As applicable, analysis results should be captured in the Hazard Tracking System (HTS).

208.3 Details to be specified. The Request for Proposal (RFP) and Statement of Work (SOW) shall include the following, as applicable:

a. Imposition of Task 208. (R)

b. Identification of functional discipline(s) to be addressed by this task. (R)

c. Desired analysis methodologies and technique(s) and any special data elements, format, or data reporting requirements (consider Task 106, Hazard Tracking System).

d. Applicable requirements, specifications, and standards.

e. Concept of operations.

f. Other specific hazard management requirements, e.g., specific risk definitions and matrix to be used on this program.