Appendix A

AIRWORTHINESS QUALIFICATION REQUIREMENTS

MANNED AIRCRAFT CREW SYSTEMS
APPENDIX A: Manned Aircraft Crew Systems

A.1 Critical Task Analysis Report

A Critical Task Analysis (CTA) of the human-system interactions shall be conducted and a Critical Task Analysis Report (CTAR) shall be prepared IAW DI-HFAC-81399. The report shall include appendices for all completed analyses (mission tasks, behavioral tasks, cognitive tasks, function allocation, information requirements, safety use cases, failed and degraded modes, and critical tasks). Each analysis shall be prepared IAW DI-HFAC-80745.

All crew control, display, and human system interfaces shall be designed and traceable to a defined set of all crew/operator required mission functions, tasks, and related activities as defined by the configuration and the intended use of the aircraft system. The CTAR shall include a comprehensive set of human engineering analyses to include mission task analysis, function analysis and allocation (human and system), behavioral task analyses, cognitive task analysis, information requirements analysis, safety use case analysis, failure and degraded modes analysis, and a critical task analysis for the aircraft system. The information requirements defined by the task and function analyses shall be designed, implemented, and traceable to the layout of all controls, displays, and the operator/crew station layout. The safety use case analyses and failure and degraded modes analyses shall be included as a part of the preliminary system safety related documentation. Updated analyses and an updated CTAR shall be prepared when changes to the configuration or intended use of the system occur, or when assumptions about the use of the system are found to be no longer valid or applicable. NOTE: Use-case analyses are insufficient means of analysis by themselves but may be included as supplemental information. Also note, all subsequent analyses are necessary to complete the Critical Task Analysis.

a. Mission Task Analysis: A mission task analysis shall be conducted. A comprehensive list of all mission based activities shall be developed and documented in support of the primary mission tasks for aviation systems i.e., Aviate, Navigate, Communicate, Subsystem Status, and Weapon Engagement, as applicable. These activities shall be broken down to include all tasks, task elements, and functions for the full range of necessary missions to be supported by the system. Based on the capability requirements, concept of operations and specific operational guidance, the full range of mission tasks shall be defined and delineated in order to ensure traceability to the system design. The results of this analysis shall be included in an appendix in the CTAR.

b. Function Analyses and Allocation: A function analysis and allocation shall be conducted IAW the aircraft system specification to describe and capture the functionality and requirements, of the system to meet the defined intended use of the system. The function analyses and allocation information shall be used to identify the full range of functions, map them to mission scenarios, identify performance requirements and limitations, delineate the functions between those designated for the human operator and those for the system, and then further
define the full range of operator tasks and task flows to be analyzed during the behavioral and cognitive task analyses. The results of this process shall be included in an appendix in the CTAR.

c. Behavioral Task Analysis: A behavioral task analysis shall be conducted to provide a basis for making conceptual design decisions. For example, before hardware fabrication, task analyses shall be considered in determining whether system performance requirements can be met by the combination of anticipated equipment, software and associated human interfaces, available personnel, and that human performance requirements will not exceed human capabilities. The time requirements for tasks shall be evaluated for task duration versus time availability, task sequencing, and task simultaneity as it relates to system latencies. The results of this analysis shall be included in an appendix in the CTAR.

Behavioral analysis breaks down each operator task down into discrete, observable, actions. The procedure for performing a behavioral task analysis is straightforward. The task shall be described as a linear sequence of observable steps and sub steps that must be executed to complete the task. Routines for operating devices, or assembly, service, and repair tasks can be given as examples for such tasks. It is typically useful to analyze skills that involve mainly overt steps.

Though traditional behavioral task analyses are often employed in the design of systems (manual and automated) and operator-aids, they do not account for cognitive processes and are less applicable than cognitive task analyses at a deeper level of design. For example, for a behavioral task analysis the steps only refer to actions; decisions are not taken into account (see Cognitive Task Analysis below).

d. Cognitive Task Analysis: A cognitive task analysis shall be conducted for all mission tasks and functions IAW the aircraft system specification. Updates shall be required when subsystems, components, or software insertions change the system configuration. In addition to the behavioral sequencing of task completion, the perceptual and cognitive elements of task completion shall be understood as they relate to workload, memory, decision making, attention, and problem solving for each mission, function, task, task element, or part thereof. The cognitive tasks for the effects of task or system feedback, the detection of system failed or degraded modes, and effects of error tolerance and/or error recovery on human performance and safety. These analyses shall consider effects of sustained and continuous operations on human performance e.g., mission duration (fatigue), environmental conditions (excessive temperatures), stress (combat), etc. The results of this analysis shall be included in an appendix in the CTAR.

The cognitive task analysis methods analyze and represent the cognitive activities users utilize to perform certain tasks. Some of the steps of a cognitive task analysis are the
mapping of the task, identifying the critical decision points, clustering, linking, and prioritizing them, and characterizing the strategies used.

Cognitive Task Analysis is used to document performance differences between novices and experts, frame the mental workload associated with complex controls and displays, describe the decision-making strategies of experts and the development and evolution of mental models, identify derived information requirements, and can also be used for troubleshooting, fault isolation, and diagnostic procedures in order to maximize human performance and minimize the occurrence of human error.

e. Information Requirements Analysis: An information requirements analysis shall be conducted IAW aircraft system specification and the results of this analysis shall be included in an appendix in the CTAR. The information requirements analysis shall distill higher level requirements and functions into the raw information elements and provide traceability between the system design and the mission task analysis, function analysis and allocation, the behavioral and cognitive task analysis, the safety use case analysis, and the failed and degraded modes analysis. The information requirements shall be modality agnostic and simply describe what information is needed and not how the information should be presented. For example, the mode of presentation shall not be dictated e.g., visual, auditory, tactile. In addition, information requirements may be derived requirements necessary to support mission tasks, task elements or functions.

Two levels (or categories) of information shall be addressed: 1) primary or sole source information, and 2) supplemental or non-primary information. It shall be noted that any information presented to the crew can or will affect their situational awareness. The information provided to the crews shall contributes to situational awareness (SA) i.e., increase SA, shall not increase operator workload, and shall not present potentially hazardous and misleading information (HMI) to the crew. The extent to which the information is accurate, timely, reliable, and usable must be understood in order to make any determination of airworthiness assessment. An information requirements analysis must be conducted based on the intended use of system and IAW aircraft system specification in order to verify performance and to identify and mitigate any potential hazards. The derived information requirements shall be evaluated for criticality, accuracy, integrity, reliability and timeliness.

The analysis should contain the following information:

1) A detailed description of the individual elements of information:

   The individual pieces of information should be described in terms of size, font, color, unit of measure, scaling, etc. (see MIL-STD-1472), and in terms of how they support specific task elements. Some of this detail may be obvious, but as the design matures the intended use of the information may not be appropriate and, thus, unnecessary (more is not always better).
2) The information format, layout, and arrangement:

How the individual elements are presented to the crews, and the layout and arrangement of the information are critical to understanding the visual search/scan patterns, and this information is vital to understanding the step 3 below.

3) An element to element comparison between the primary source and the secondary display:

This comparison affords insight into transitions between a primary information display and the secondary display. The reasons for transitions are not necessary; however, if the information is within the direct line-of-sight of the crew, then it can be assumed that attentional focus may not be on the primary system at the appropriate time.

4) A description of the dynamic behavior between and among elements, including timeliness (total system latencies):

Prior to modeling and validation, this step is necessary to understanding how the display of information will change over time or move. Dynamic behavior must be modeled in order for designs to be understood, and the relative timeliness of information must be defined to understand impacts on human performance and task success.

5) A description of exceptions and new, novel, or non-traditional means of presenting specific elements (or sets of information e.g., symbols and the symbology set):

A specific category of the analysis is how and where the design varies from a standard design approach. When assumptions are violated, when traditional means of presentation are not used, or when new or novel information formats, layouts, arrangements, or dynamic behaviors are used, there must be a clear description of those exceptions. Exceptions typically drive validation test points to ensure the modifications to the design can be understood and do not cause confusion, misunderstanding, or higher operator workload.

f. Safety Use Case Analyses: A safety case analysis shall be conducted as the basis for the system safety program. The safety use case analysis is a breakdown of the critical tasks related to operating the system as intended in its expected environment. Each use case shall be defined based on the evolution of the task analysis, functional allocation, and the availability of mitigating functions based on the system configuration e.g., aircraft system. The use case outlines the tasks, activities, functions, timeline(s), assumptions and dependencies related to the execution of each of the critical tasks (to include critical phases of
flight and other safety related factors, as applicable) and the results of this analysis shall be included in an appendix in the CTAR.

g. **Failure and Degraded Modes Analysis:** A system level failure and degraded modes analysis shall be conducted IAW aircraft system specification. The program is responsible for identifying those design characteristics or procedures which may contribute substantially to human error and shall propose corrective action. All failure conditions shall be differentiated between failures of equipment alone, failures resulting from human-system incompatibilities, and failures due to human error. Human errors occurring in the performance of critical tasks shall also be analyzed to determine the reason for their occurrence. How individual failures or degraded modes of operation are identified, propagated through the system, and subsequently displayed to the crews will have a dramatic impact on situational awareness, especially if not handled appropriately.

All possible system, subsystem, and component failed and degraded modes shall be included as appendices in the CTAR and describe where those failed and degraded modes occur, how they occur, how those failed and degraded modes propagate through the system, how the failed or degraded modes are presented to the crew, and what mitigations are available for any given failure or degraded condition (subject to validation). Prioritization, automatic response (declutter, blanking, etc.), and other related system alerting shall be discussed, as appropriate.

h. **Critical Task Analysis (CTA):** A critical task analysis shall be conducted IAW the aircraft system specification and prepared IAW DI-HFAC-80745 to include the following:

1) Information required by operator or maintainer, including cues for task initiation;
2) Information available to the operator;
3) Information processing and decision evaluation process;
4) Possible decisions that could be reached;
5) All possible actions that might be taken depending on the decision reached;
6) Body movements required by all actions that might be taken;
7) Workspace envelope required by all actions that might be taken;
8) Workspace available;
9) Location and condition of the work environment;
10) Frequency and tolerances of all actions that might be taken;
11) Time available for completion of the task;
12) Feedback informing operator of the adequacy of actions taken or the failure to take an action;
13) Tools and equipment required, and their timely availability;
14) Number of personnel required, their skills, and aptitude requirements;
15) Probability and severity of human error;
16) Potential for error recovery;
17) Job aids, training, or references required, and their timely availability;
18) Communications required, including type of communication;
19) Hazards involved;
20) Personnel interaction where more than one person is involved;
21) Performance limits of personnel;
22) Operational limits of hardware and software and associated user interfaces;
23) Concurrent tasks and the associated potential workload and attention management issues.

The critical task analysis shall include all affected operational missions and phases of flight including failed and degraded modes of operation. Operator problem areas that might adversely affect mission accomplishment or flight safety/airworthiness and so proposed corrective action(s) shall be identified.

Analyze and verify that each design element is traceable to a specific task, task element or system function. Analyze the information requirements defined in the task analyses and verify that there is traceability to design elements that are implemented in the layout of all controls, displays, and the operator/crew station.

Analyze the information requirements defined in the CTAR to determine that they accurately reflect the configuration, intended use, and any assumptions concerning the use of the system.

A.2 Human Engineering Program

A.2.1 Operator Workload Program
The aircraft system shall have an Operator/Crew Workload Program to ensure safe flight. An analysis of the full range of crew/operator missions, tasks, functions and scenarios shall be conducted to identify all high workload segments and tasks based on the CTAR. Operator (individual and crew) workload analyses shall be performed and compared with performance criteria. To avoid overloading or under loading, the degree to which demands of any task or group of tasks tax the attention, capacities, and capabilities of system personnel (individually and as a team) and thus affect performance workload must be evaluated. Sensory, cognitive, and physiological limitations shall be considered, as applicable. The workload analyses shall define operational sequences and task times. Preliminary workload estimates shall correlate required actions with crew and mission based tasks for each task component (visual, auditory, motor, and cognitive) specified in terms of time, workload, mental effort, and psychological stress. A workload estimate for each individual shall be defined in a fashion permitting individual and crew workload to be related to operational procedures. A Human Engineering Workload Analysis Report shall be prepared IAW DI-HFAC-80745.

Concurrently, a simulation concept based on the aircraft system configuration shall be developed to ensure that estimates of operator workload can be determined prior to flight test activities. A Human Engineering Simulation Concept shall be prepared IAW DI-HFAC-80742. The simulation concept shall enable the assessment of crew/operator
workload using actual flight hardware and through simulation for the full range of operator missions, tasks, and functions. Any simulation shall represent the integrated system as it regards human-in-the-loop, situational awareness, crewstation or operator station geometry, controls, displays, display software, and aircraft and payload performance.

A Workload Assessment Test Plan shall be prepared IAW DI-HFAC-80743 based on an analysis of missions (including emergency procedure situations) as defined in the CTAR and the Human Engineering Workload Analysis Report. The test plan shall cover the system configuration under test and additional test plans shall be prepared for each subsequent modification to the system configuration, as appropriate, or when the intended use of the system changes.

Specific methodology and threshold criteria for acceptable workload shall be tailored based on the system configuration and its intended use, as well as thresholds for human performance of critical tasks e.g., not to exceed a ‘4’ using the Modified Bedford Workload Rating Scale, or equivalent method, for any individual, task, function or segment thereof whereby there is still sufficient attentional capacity to attend to other easy tasks. Note, other acceptable methods may be used i.e., Subjective Workload Assessment Technique (SWAT), National Aeronautics and Space Administration Task Load Index (NASA TLX), etc. in order to increase accuracy and generalizability of the results.

Human Factors Workload Assessment(s) shall be conducted in accordance with human factors workload assessment test plan(s). The results of each workload assessment shall be prepared IAW DI-HFAC-80744, a Human Factors Workload Assessment Test Report. A baseline workload assessment shall be conducted with the initial aircraft design. All subsequent workload evaluations shall use the comparative baseline as a measure of determining changes in workload based on the changes in the system configuration as the system matures, is upgraded, etc. Each assessment shall be holistic in nature while conducting representative missions with current concepts of operations and using adequate, and appropriate sample sets.

Holistic workload evaluations shall ensure that no individual mission, task, function or segment thereof creates conditions whereby tasks shedding occurs. While it is acceptable to specify a higher ‘maximum’ workload (e.g., a ’5 or 6’ on the Bedford Workload Scale), it is imperative that a baseline for specific critical tasks is set at a lower threshold such that during high stress emergency conditions the critical tasks can still be performed and those tasks are not at risk of being shed at an inappropriate moment. Setting a higher baseline ‘maximum’ workload rating value creates the risk that critical tasks can no longer be performed during emergency or critical phases of flight. Any workload increase during critical phases of flight shall be considered a MAJOR safety effect.

Workload Assessments shall be performed using a representative sample of crew/operator mission segments and tasks and evaluated in part- and full-mission
scenarios, to include, as a minimum, any segment, task, or part thereof, that may present excessive workload. All workload evaluations shall be conducted using representative operational users from a broad range of experience with a sample size sufficient to produce statistical power necessary to make generalized conclusion about the result. A minimum of seven (7) Government crew/operators will participate in each assessment. A workload assessment shall be performed to verify the ability of the crew to accomplish all critical tasks identified in the task analysis, transition between tasks, and perform multiple concurrent tasks within the time and accuracy constraints imposed by the mission and within specified workload levels. A quantitative estimate of the crew workload in each segment or task shall be made. A representative sample of “mission segments,” shall include any segments/tasks that might have excessive workload. Workload assessments shall also ensure that all normal and emergency procedures can be accomplished within workload limits.

Identified excessive workload segments and tasks shall be tested as part of a holistic assessment of workload during flight in order to validate workload estimates. Ensure that crew/operator preliminary workload estimates that were identified in simulation(s) are also assessed during developmental and operational flight test activities. All workload assessment reports during flight test operations shall be prepared IAW DI-HFAC-80744, Human Engineering Flight Test Report.

Additional Human Factors Workload Assessments shall be conducted, as applicable, when changes in the configuration of the aircraft system impact task or mission flow, processes or crew coordination activities, or when new, modified, or changes in operator functions are implemented.

A.2.2 Situational Awareness Program
The aircraft system shall have an Operator/Crew Situational Awareness Program to be run in parallel with an Operator/Crew Workload Program.

As defined in MIL-HDBK-516, Situational awareness (SA) is the ability to identify, process, and comprehend critical, perceived elements of information in one’s environment in order to make decisions about a future state and/or needed actions. Any information that is presented to the crew can or will affect situational awareness. See MIL-HDBK-516.

Any information that is presented to the operator/crew can, or will, affect situational awareness. If a system or information is presented 'for situational awareness', then performance must be demonstrated to prove that the information or system contributes (increases situational awareness), does not increase workload, or present potentially hazardous and misleading information. The information presented during operational sequences and task times shall not potentially present hazardous or misleading information or create distractions or other losses of attentional focus necessary to complete the mission safely. Information presented to the crew shall be of sufficient integrity to perform the intended use without producing false or hazardously misleading information.
An analysis of operator (individual and crew) situational awareness shall be conducted and compared with performance criteria. A Human Engineering Situational Awareness Analysis Report shall be prepared IAW DI-HFAC-80745. To avoid any degradation in operator/crew Situational Awareness, the degree to which information presented to the crew may adversely influence perception, comprehension or subsequent decision making of critical situations shall be included. Sensory, cognitive, and physiological limitations shall be considered, as applicable.

Prepare a Human Factors Situational Awareness Assessment Test Plan prepared IAW DI-HFAC-80743. The test plan shall cover the system configuration and the test shall be conducted for each subsequent modification to the system configuration or when the intended use of the system changes. The test plan shall be developed based on an analysis of missions (including emergency procedure situations) as defined in the CTAR and all applicable Human Engineering Workload Analysis Reports.

Specific methodology and threshold criteria for acceptable Situational awareness shall be tailored based on the system configuration and its intended use, as well as thresholds for human performance. If a system or any element of information is presented to the crew ‘for situational awareness,’ then performance shall be demonstrated using the Situational Awareness Rating Technique (SART), Situational Awareness Global Assessment Technique (SAGAT), or equivalent method, to establish that the information presented to the crew contributes to SA (increases SA), does not increase operator workload, and does not present potentially hazardous and misleading information to the crew. Note, it is fundamental that the questions asked during any assessment for situational awareness are appropriate, and at a level of decomposition to ensure that crew and operator situational awareness was maintained or enhanced. Questions that are too broad in nature cannot identify if there were periods of degraded or loss of SA.

A Situational Awareness Assessment shall be conducted IAW Human Factors Situational Awareness Assessment Test Plan and a Human Factors Situational Awareness Test Report shall be prepared IAW DI-HFAC-80744 to documents the results of the assessment. This report shall also be included and updated as part of the Human Engineering Program Test Report. The Situational Awareness Assessment shall be performed in conjunction with an Operator Workload Assessment using a representative sample of crew/operator mission segments and tasks and evaluated in part- and full-mission scenarios, to include, as a minimum, any segment, task, or part thereof, that may adversely affect crew Situational Awareness. A minimum of seven qualified Government crew/operators, with various experience levels, will participate in this assessment.

A Situational Awareness Assessment shall be performed to verify the ability of the crew to accomplish all critical tasks identified in the task analysis, transition between tasks, and perform multiple concurrent tasks within the time and accuracy constraints imposed by the mission and within specified workload levels. A quantitative estimate of the crew
Situational Awareness in each segment or task shall be made. A representative sample of “mission segments,” shall include any segments/tasks that might have an adverse impact on Situational Awareness.

All Situational Awareness evaluations shall be conducted using representative operational users from a broad range of experience with a sample size sufficient to produce statistical power necessary to make generalized conclusion about the result. Human Factors Workload Assessments shall be conducted, as applicable, in conjunction with all Situational Awareness Assessments in order to correlate the relationship between Situational Awareness and Operator Workload when changes in the configuration of the aircraft system impact task or mission flow, processes or crew coordination activities, or when new, modified, or changes in operator functions are implemented.

Test and verify the full range of crew/operator missions, tasks, functions and scenarios have been analyzed to establish that operator/crew Situational Awareness has not been degraded and that the information does not present potentially hazardous or misleading information.

Test and verify crew/operator Situational Awareness has been validated through actual flight hardware and through simulation for the full range of operator missions, tasks, and functions. This simulation shall represent the integrated system as it regards human-in-the-loop, situational awareness, crewstation or operator station geometry, controls, displays, display software, and aircraft and payload performance.

Test that crew/operator preliminary workload estimates that were evaluated in simulation(s) are also assessed during developmental and operational flight test activities. Situational Awareness shall be evaluated in flight to establish that the information presented to the crew contributes to SA (increases SA), does not increase operator workload, and does not present potentially hazardous and misleading information to the crew. The report for all of Situational Awareness assessments conducted during flight test operations shall be prepared IAW DI-HFAC-80744, Human Engineering Flight Test Report.

Additional Human Factors Situational Awareness Assessments shall be conducted, as applicable, when changes in the configuration of the aircraft system impact task or mission flow, processes or crew coordination activities, or when new, modified, or changes in operator functions are implemented.

A.3 The Airworthiness Process Framework for the Qualification of Autonomous Systems
This paper communicates four stages of application of the proposed Framework in the airworthiness process:
1) The fundamental process of task and function analysis and allocation
2) Determination of the type of autonomy
3) Determination of the level of autonomy
4) The consequences of process outcomes

The framework’s language and structure will be used to drive and inform system safety in the acquisition process by facilitating analysis of the criticality of certain tasks and functions, as well as the risks and potential consequences associated with architecture and design decisions made early on. All in all, this whitepaper will address these issues within the context of human performance, machine autonomy, and airworthiness.

A.3.1 Stage One: Mission, Task and Function Analyses and Allocation

Every structure starts with a foundation. In this vein, the process framework begins with applied system engineering. All crew controls, displays, and human system interfaces for functions must be designed and traceable to a defined set of all crew/operator required mission functions, tasks, and related activities as implied by the configuration and the intended use of the aircraft system. Within the evolving acquisition process, the Critical Task Analysis and the subsequent CTAR is the preferred method by the U.S. Army Combat Capabilities Development Command Aviation & Missile Center to provide a comprehensive documented set of analyses that include mission, task, and functional analyses. These should then be allocated between the human and the autonomous aspects of the system. This analysis and allocation of tasks and functions is supported by human behavioral and cognitive task analyses in order to form the basis for requirements development. As the system evolves, the safety use case analyses and the failure and degraded modes analyses form the basis for understanding the consequences and severity of failures, which are used to establish the functions’ criticality within the system as a basis for the system safety classifications. This is not new. However, the complexities of autonomous functions demands rigor and the basis for that is the comprehensive analysis and classification of the desired system functions. The result of this collection of works drives the Critical Task Analysis for the aircraft system. The following analyses derived from MIL-STD-46855 all play a vital role in the development of a complete CTAR:

**Mission Task Analysis:** A mission task analysis is conducted based on the configuration and the intended use of that system within the scope of the Concept of Operations (CONOPS). A comprehensive list of all mission based activities can be developed and documented in support of the primary mission tasks for aviation systems (i.e., Aviate, Navigate, Communicate, (managing) Subsystem Status, and Weapon Engagement). These activities are then broken down to include all tasks, task elements, and functions for the full range of necessary missions to be supported by the system. Based on the capability requirements, concept of operations and specific operational guidance the full range of mission tasks must be defined and delineated in order to ensure traceability to the system design.

**Function Analyses and Allocation:** The system engineering approach described here calls for a function analysis and an allocation process to identify the full range of functions, map relationships to/from mission scenarios, identify performance requirements and limitations, and to delineate the functions between those designated for the human operator and those for the system. Although the human is part of the
‘system’, for purposes of this whitepaper we delineate those tasks allocated to the human as separate from those assigned to the machine. Regardless of whether any function is allocated to man or machine, additional levels of detail are necessary. While the allocation step is typically conducted as part of the functional analysis, with regard to autonomy the allocation of tasks goes a step further, in that both the type and level of autonomy must be defined (see below).

**Behavioral Task Analysis:** A behavioral task analysis based on the performance of the function(s) is required where the analysis is needed to provide a basis for making conceptual design decisions and used as the basis for logical derivations of task criticality based on expected or intended levels of human interaction. This is a direct corollary to the level of automation selected. While autonomous behavior suggests it is the machine and not the human performing the action, it is still critical to understand human interaction with the aircraft environment.

Control interfaces, overrides, time to criticality (required timeline to provide the ability to respond appropriately to a situation), and related factors are tied directly to the human response characteristics. For example, before hardware fabrication, task analyses must be considered in determining whether total system performance requirements can be achieved by the combination of anticipated equipment, software and associated human interfaces, available personnel, and that human performance requirements will not exceed human capabilities. The time requirements for tasks must be evaluated for task duration versus time availability, task sequencing, and task simultaneity as it relates to system latencies.

Behavioral analysis breaks down each operator task into discrete, observable, actions. The procedure for performing a behavioral task analysis is straightforward. The task shall be described as a linear sequence of observable steps and sub steps that must be executed in sequential order to complete the task. Routines for operating devices, or assembly, service, and repair tasks can be given as examples for such tasks. It is typically useful to analyze skills that involve mainly easy to observe steps.

Though traditional behavioral task analyses are often employed in the design of systems (manual and automated) and operator-aids, they do not account for cognitive processes and are less applicable than cognitive task analyses at a deeper level of design. For example, for a behavioral task analysis the steps only refer to actions; decisions are not taken into account (see below).

**Cognitive Task Analysis:** A cognitive task analysis is conducted for all mission tasks and functions for the aircraft system, and should be updated when subsystems, components, or software insertions change the fundamental system configuration. In addition to the behavioral sequencing of task completion the perceptual and cognitive elements of task completion need to be documented and understood as they relate to workload, memory, decision making, attention, and problem solving for each mission, function, task, element, or part thereof. The cognitive tasks for the effects of task or system feedback, the detection of system failed or degraded modes, and effects of error
tolerance and/or error recovery on human performance and safety must be understood within the context of system performance. These analyses shall consider effects of sustained and continuous operations on human performance e.g., mission duration (fatigue and vigilance), environmental conditions (excessive temperatures), stress (combat), etc.

The cognitive task analysis methods analyze and represent the cognitive activities that are needed to perform certain tasks. Some of the steps of a cognitive task analysis are the mapping of the task, identifying the critical decision points, clustering, linking, and prioritizing them, and characterizing the strategies used.

The cognitive task analysis is used to document performance differences between novices and experts, frame the mental workload associated with complex controls and displays, describe the decision-making strategies of experts and the development and evolution of mental models, identify derived information requirements, and can also be used for troubleshooting, fault isolation, and diagnostic procedures in order to maximize human performance and minimize the occurrence of human error.

A good descriptive example for tasks understood by those who drive automobiles is provided by the U.S. Department of Transportation (2006). The report describes tasks that many would understand for both behavioral and cognitive aspects of the task based on applicable safety use cases, and in a way that can generally be understood by this audience. The report details much of what many of us do while driving on any given day, but things that we don’t normally actively think about. Much of it might appear to be common sense, yet when not described or delineated to the level the report provides it might be easy to skip over, omit or assume elements that would otherwise change the perception of the environment, or a critical factor in decision-making in real time, and perhaps ultimately change the outcome.

**Information Requirements Analysis:** The information requirements analysis is used to distill and understand the raw information elements for any autonomous function in order to provide traceability between the system design and the mission task analysis, the function analysis and allocation of tasks and functions, the behavioral and cognitive task analyses, the safety use case analyses, and the failed and degraded modes analyses. The definition of information requirements predate design decisions, and therefore do not consider the mode of presentation (e.g., visual, auditory, tactile) and should not be dictated prior to a design decision. In addition, it is important to note that information requirements may be derived requirements necessary to support mission tasks, task elements or functions that are not otherwise explicitly stated. The information requirements should also include assumptions and dependencies that other pieces of data or information will be available when needed.

Any information presented to the crew can or will affect their situational awareness. Thus, it is critical to establish that the information provided to the crews contributes to situational awareness (SA) i.e., increases SA, but also does not increase operator workload, or present potentially hazardous and misleading information. The quality of
the information must be characterized to ensure that the information is accurate, timely, reliable, and usable. An information requirements analysis must be conducted based on the intended use of the system in order to verify performance and to identify and mitigate the inherent risks. The derived information requirements can then be evaluated and documented for validity, accuracy, integrity, reliability, latency, continuity, and as appropriate, readability. These factors are not only critical for human consumption of information, but also for the design and implementation of automated system behavior and the display of information based on the type and level of autonomy.

**Safety Use Case Analyses:** As the system design matures, the safety case analysis is conducted and documented as part of the system safety program. The safety use case analysis part of the holistic safety case analysis. It is a breakdown of the critical tasks related to operating the system as intended in its expected environment. Each use case is defined based on the evolution of the task analysis, functional allocation, and the availability of mitigating functions based on the system configuration, e.g., the aircraft system, and ultimately the criticality of the function. The use case outlines the tasks, activities, functions, timeline(s), assumptions and dependencies related to the execution of each of the critical tasks (to include critical phases of flight and other safety related factors, as applicable) and the results of this analysis must be documented in appendices in the comprehensive CTAR. The outcome of the system safety analysis is the basis for the functional hazard assessment and the risks related to human system interaction.

**Failure and Degraded Modes Analysis:** A system level failure and degraded modes analysis is a mechanism for understanding the safety cases. The system, either by design or consequence, will fail or degrade based on the expected reliabilities in system performance. However, more robust measures must be applied to non-deterministic functions, to include the human. The intent of these analyses is to identify the design characteristics or procedures which may contribute substantially to human error in order to propose mitigations or corrective action. All failure conditions need to be differentiated between failures of equipment (hardware, software, etc.) alone, failures resulting from human-system incompatibilities, and failures due to human error (i.e., errors of omission and commission). Human errors occurring in the performance of critical tasks must also be analyzed to determine the reason for their occurrence. How individual failures or degraded modes of operation are identified by the system, propagated through the system, and subsequently displayed to the crews will have a dramatic impact on situational awareness, even if handled appropriately, and certainly if not handled properly.

The failure and degraded modes analyses are needed to describe where those failure and degraded modes occur, how they occur, how those the modes propagate through the system, and the failed or degraded modes are presented to the human operator. This is necessary so that mitigations can be engineered for each given failure or degraded condition.
Critical Task Analysis: This the pinnacle analysis in stage one of this process. The critical task analysis uses the output of all the other analyses to identify those tasks and functions that are critical to safe operations. The selection of critical tasks without the aforementioned analyses should not be used as a shortcut to system engineering, but as the last step in a structured, systematic, and repeatable process to define the task elements. This analysis should include the following:

1. Information required by human (or the system), including cues for task initiation.
2. Information available to the human or system.
3. Information processing and decision evaluation process.
4. Possible decisions that could be reached.
5. All possible actions that might be taken depending on the decision reached.
6. Frequency and tolerances of all actions that might be taken.
7. Time available for completion of the task.
8. Feedback informing the human of the adequacy of actions taken or the failure to take an action.
10. Potential for error recovery.
11. Job aids, training, or references required, and their timely availability.
12. Communications required, including type of communication.
13. Hazards involved.
14. Personnel interaction where more than one person is involved.
16. Operational limits of hardware and software and associated user interfaces.
17. Concurrent tasks and the associated potential workload and attention management issues.

The summary CTAR must address each task/function separately and include all affected operational missions and phases of flight, including for all known degraded modes of operation. Each critical task should be analyzed to a level sufficient to identify operator problem areas in addressing failure or degraded operations that might adversely affect mission accomplishment or flight safety/airworthiness so proposed mitigations or corrective action(s) can be developed and evaluated.

It is important that at the end of the analysis and allocation process it is possible to verify that each autonomous design element is traceable to a specific task, task element or system function. The flow of analyses described above are independent but also interrelated pieces of the process that are necessary en total to fully understand the task or function, how it is allocated to either man or machine, what is the criticality and consequences of failure if not performed correctly.

A.3.2 Stage Two: Defining Types of Autonomous Functions
The next stage of the process is classifying the type of the function that an autonomous system provides. Leveraging the work of Endsley and Kaber (1999) and Parasuraman, Sheridan and Wickens (2000), there are four specific types of interactions between
autonomous components and the systems in which they reside: Sensory Processing (input), Perception/Working Memory, Decision Making, and Response Selection/Execution. While these are put into psychological terms, the authors expanded those types into a four stage model for human information processing. An expanded version is as follows:

**Type 1: Information Acquisition or Monitoring**
The type of autonomy here is focused solely on the acquisition of the raw data that will be used (by either the system or the human) to conduct the necessary tasks (Parasuraman, et al, 2000). It could include the use of databases, datalink communications, or even sensor-based inputs. Regardless, Endsley and Kaber (1999) also expanded the concept the ‘monitoring’ or the process of seeking the data needed to support a task.

**Type 2: Information Analysis or Processing**
This is where the raw data is processed into something meaningful, whether the information is directed to the machine or the human (Parasuraman, et al, 2000). Endsley and Kaber (1996) used the term ‘Generating’ [as in generating information, creating meaning from the raw data]. Here the data that has been acquired is processed into a usable form. The raw data is collated and/or processed to have some meaning usable by the human, the system, or both.

Here the raw elements of information are combined, distilled, transformed, or otherwise manipulated for the purposes of task completion. It is important to note here that an autonomous system could have one or more types of autonomy. For example, the same autonomous system could acquire, or store needed information, and may also process that data for later use.

**Type 3: Decision and Action Selection**
Type 3 interaction assumes that data has been acquired and into some meaningful form. Thus, the next step is to decide what to do with it. In a type 3 autonomous system, the system is designed to select the appropriate response(s) based on the tasks or function it was intended to support. Parasuraman, et al (2000) pointed out that here an action has been selected (i.e., a decision has been made), but it does not mean that the system is designed to implement the selection.

**Type 4: Action Implementation**
The first three types of autonomy map directly to the airworthiness qualification process of understanding the data (and source), the processing of that data, and the subsequent display of information, whereby each is understood and qualified independently in order to understand the holistic quality of information in the system. The last type of autonomy, however, has been traditionally reserved for the human: the implementation of action.

It is vital that the quality of the data is understood in terms of potential inherent errors that can propagate through the system. So too is the importance of the processing of
the data, and of being able to characterize the accuracy, integrity, reliability, availability, continuity and timeliness of the data when it is transformed into meaningful units (either to the human or to the machine). Tradition human engineering focuses on the display of that information based on the quality of the data and process that proceeded it, but within the realm of autonomy we not only have to explore the display of that information, but also the quality of the action.

With the advent of highly autonomous functions, the response or implementation of some action (whether human or machine) must now also be characterized. As such, this framework must accommodate the system response and assist in the quantification of probability of failure that was otherwise difficult to assess when the human operator was the sole respondent.

A.3.3 Stage Three: Defining Levels of Autonomy
Autonomy is often thought of as an all or nothing approach to system design. Often it is stated that a system is ‘fully automated’, or perhaps that it is a “fully autonomous” system, without any regard to what task, function, or segment therein is actually automated. This generic labeling of autonomous activity is over-simplifying a far more complex set of levels of interaction.

While the SAE and the automotive industry has adopted a simpler five (six) stage delineation of levels of autonomy not dissimilar that that proposed by Ensley (1987 and 1996), it did not provide sufficient discrimination for a wide variety of complex interactions between man and machine. First proposed in 1978, Sheridan and Verplanck offered ten increasing levels of autonomy from pure manual controls systems to the pinnacle, the fully autonomous system. However, short of the last level (fully autonomous) there was always a level of human interaction expected or implied. This model was further elaborated on by Endsley in 1999, by Parasuraman, Sheridan and Wickens (2000), and adapted for use in robotics by Beer, Fisk and Rogers (2014).

Therefore, the following levels are a derivation leveraging the logic and language from all of these previous efforts. The framework itself was derived directly from the work of Parasuraman et al, and the larger framework depiction can be found in Enclosure A. The levels described herein, therefore, have been merged together and the language has been slightly expanded in order to facilitate easy categorization of a ten level taxonomy within the derived framework. The merger was a result of the intent to include both behavioral (Sheridan and Verplanck, 1978) and cognitive responses (Endsley and Kaber, 1996) to defined levels of human-system interaction so that the classification of the level of automation is clear.

**Level 1: Manual Control**
The system offers no assistance to the human operator. The human has to acquire information, process it, make a decision and implement it without the system helping. The human must make all decisions based on information observed, perceived, self-generated, selected or extrapolated from what is available and then physically carry out the response action. This is the lowest level of automation and workload tends to be
higher, but also situational awareness because the human is an active participant in system performance and task outcome. This is the traditional system design where the human must perceive the environment, process the meaning of those elements, understand what that means, decide on a course of action, and then implement action to accomplish those actions.

**Level 2: Simple Automation**
The system here provides a complete set of options for implementation or action alternatives. It would still be possible here for the human to add additional options to the set and the human would still be executing most of the control actions. Regardless of the type of autonomy, here the system provides options. It does not prioritize or offer a ‘best’ solution. It simply provides a list of alternatives. The human can add or modify the list of options, but ultimately the decision and action selection is up to the human.

**Level 3: Automated Functions and Batch Processing**
At this level, the system narrows the possible list of alternatives or options down to a few. Because there is an implied process of refinement, the list may even be comprised of the best available options and not just a laundry list of possibilities. In some cases, this could also be the level where the human generates and/or selects options that are then turned over to the system to implement specific subroutines, but not to the extent where the human relinquishes control of the system to make automated control actions. This is still a low level of automation because the human is the decision maker, but it defers some action to the system when the human fully understands what actions are being done, how they are being done, and when they are being done. These are going to be typically administrative, clean up, or maintenance type tasks and not used for critical tasks.

**Level 4: Shared Control**
The system down selects from a larger list of options based on established criteria and provides the ‘best’ option as a recommended response or action to implement. Both the human and the system can still create alternative options, but again the human still makes the final decision on which to implement and would be responsible for providing the control action/command. This level is where trust in automation may start to become critical. If the operator cannot trust the recommended solution it will be nearly impossible to proceed or expand to higher levels without trust.

**Level 5: Decision Support**
The next step in the progression of autonomous functions would then be for the system to actually implement the recommended action, but the human still makes the decision to implement and then permits the system to take action. The system generates options, the human selects the option, and then the system implements the decision. This term is used generally to perform tasks requiring time and/or for tasks that create higher workload for the human to generate a result independently and where a computer is perhaps better suited to do the work.

**Level 6: Blended Decision Support**
Here the system makes a selection and will perform the action after a given time period designed to give the human the time to cancel or override the action before the system can implement it. The system generates the options, selects the ‘best’ option, then executes it but the human must consent. Here the human could also override the system choice and select another option, but the system still performs the action. Ultimately, this is intended to reduce workload, but the risks related to the criticality of task execution is dependent the visibility and the time allotted for the human to perceive, comprehend and decide to accept or reject the system select response.

Level 7: Rigid System
The system performs the action without any human consent, but the system does inform the human what it did. The system provides a set of options and the human still has to select one of them. The system then performs the action in a timely manner and it clearly communicates the action selected, and the appropriate modes and other annunciations to the human to facilitate situational awareness. While technically a bridge to the next level, the Rigid System, does not allow the human to change or add input to the list of options.

Level 8: Automated Decision Making
The system performs the action without the human, and only informs the human if the human asks. The system selects and carries out the selection. However, unlike the Rigid System, the human can still provide inputs to the options. And, unlike Blended Decision Support, the human cannot provide another option. Here the human is responsible for establishing modes and awareness of automated actions and selection by querying the system. Workload is typically low when everything works as intended. However, this level may lead to significantly lower situational awareness and at this stage it becomes increasingly difficult and higher workload should be anticipated if the human is expected to facilitate recover from a failed or degraded mode of operation. In addition, inappropriate or misguided system responses due to inadequate, erroneous or otherwise poor designs is considered a separate category of error. The criticality of the task or function will drive much higher reliability rates to ensure safe operation.

Level 9: Supervisory Control
Again, at this level the system performs the action, but it only informs the human if the system decides to. The role of the human is to monitor system status and to intervene only when necessary. This fundamentally changes the way the human and system interact as the human is no longer an active participant but a completely passive observer until an undesired response or outcome is identified. This tends to create low workload conditions while everything is working, but also, to lower situational awareness at the same time. Again, when/if the human is expected to recover from an error, there is an assumption that the human has the information and control surfaces available to perceive and comprehend the situation in order to make effective action selections and subsequent control inputs to remedy it. Reliability factors are increasing again because the system cannot rely on the human as a mitigator to unknown or unpredicted failures or degraded modes of operation.
**Level 10: Full Automation**
The system decides everything concerning the task or function. It can act completely autonomously, and in short, can ignore the human operator. The system carries out all functions, including failed and degraded modes, but only in so much as it was programmed to do so. While this is the level of unmanned operations, the risks and consequences change without the human in the loop. This will have the highest levels of reliability and traditional mitigations to use the human for detection is not available, and the cost of human intervention would be at extremely high workload at times where the human has the lowest possible situational awareness because they have been a passive observer at best and vigilance, attentional focus and other factors will impede optimal response and performance.

**A.3.4 Stage Four: Consequence of Failure**
Task criticality and the consequences of failure

Ultimately, whether a task should be automated should be based on the consequences of failure. Deciding to automate any function should be weighed against the potential risks of the outcome had it not been automated. This determination of risk is part of the airworthiness process. Thus, establishing the consequences of failure is a critical component for transitioning the taxonomy and classification of autonomous functions to a safety process. This dynamic evolution and the changing nature of human interaction with different levels of autonomy must be understood and documented as part of the system design. In order to understand potential errors and undesired outcomes the consequences of failure need to be understood with respect to both the human operator (primary consequences) and the system as a whole (secondary consequences). Thus, this part of the framework is intended to communicate the significance of transferring control to a system that in some cases will increase performance, lower workload, and possibly improve situational awareness overall but in other cases create confusion and a loss of situational awareness, or disrupt performance or workload due to an abnormal situation or system response. Additionally, the consequences can be understood in terms of system reliability requirements and tangible (loss of life, damage to equipment, etc.), and intangible costs (loss of trust). We discuss both of these in a little more detail below.

**Primary:** Relationship with workload and SA
What the system needs is the same as the human needs to do the same thing. Having said this, it is clear that in many cases automation can actually result in significant reductions in the occurrence of human error. And several studies highlight that when the system is working as expected operator workload is often reduced. These are the desirable outcomes, but not especially focused on identifying the impacts to the human operator when things don’t go according to plan. Primarily, what is the relationship between workload and situational awareness as one progresses through each of the levels of autonomy?

Endsley (1993) points out that there may actually be a level of independence between workload and situational awareness. This is reflected in the asymmetry in changes in
workload as SA as the level of autonomy increases. But Endsley (1996) elaborated on this thought and suggested that adverse effects on SA and workload at higher levels was due to the fact that at higher levels of automation the problem becomes an ‘out-of-the-loop’ performance problem. In these situations, humans tend to take more time to detecting problems and subsequently responding to them in an appropriate manner. Endsley also suggested that the consequences of this range from slight delays in human response all the way to catastrophic failures.

The effect on workload as one progresses into the higher levels of autonomy changes in the sense that the quality rather than the quantity of workload is affected. As the human progresses up through the levels of autonomy from manual control to supervisory control workload evolves from an active control operation to be a passive observer that now monitors the performance of numerous subroutines and related functions that are maintaining the system. The human’s understanding of the system changes (mental schema) with autonomous behavior in order to understand, predict, and manipulate their behavior. (Sarter, Woods, and Billings, 1997). This dependency with vigilance must be understood, especially with regard to any expectation for the human to respond (take-over) or otherwise intervene.

Essentially, human pattern recognition (information processing) needs to become more efficient at higher levels of autonomy in order to maintain cognizance of what the system is doing, but this may also lead to blind sports or lapses in human performance when patterns do not present in the traditional way, or when the evolution of the pattern is inconsistent, abnormal or otherwise erratic (skips steps, jumps to a recommendation/selection where the human is not privy to the information used to make the selection, expected order of behavioral steps seems awkward or out of sequence, etc.) which leads to uncertainty, undiagnosed failures, and issues with trust (see below). All of these factors, to include task vigilance, all lead to potential layers of human error, or varying degrees where the human would be unable to perceive and or respond to failure conditions. These consequences need to be clearly understood and articulated as part of this process.

**Secondary:** System reliability, trust, and cost of outcome
Obviously, as the level of autonomy increases the expected reliability of the system must increase as the consequences of failure become increasingly difficult to mitigate or overcome. This has a direct impact on development costs. Secondary consequences also tend to align with traditional methods of defining functional hazards in terms of the derived severities and the predicted probabilities of failures, as well as other performance factors that must be understood in purely acquisition terms (loss of life, damage to equipment, etc.). In this aspect, there is a direct link to the current safety processes. What is missing, however, and articulated by the IMPACT Study is how to tie the human operators (a deterministic factor) to the probabilistic nature of system safety. This will be explored in a subsequent whitepaper to attempt to link this framework to ongoing efforts to expand the safety and risk management process (i.e., SMTP, etc.) Regardless, secondary consequences must also be documented, as they
are understood, such that the transition to system safety documentation can be achieved.

The other secondary consequence of design is trust in the automation itself. Trust, while a human concept, is also considered a secondary consequence for the simple reason that if the system cannot be trusted, it will not be used. Parasuraman et al (2008) suggested that the construct could be a predictor of dependence on automation, and other related design criteria such as whether the system could accommodate a human operator who demanded the option to override the system at any given moment. Low levels of trust lead to misuse or perhaps not using the system as intended. High levels of trust may lead to lower situational awareness and workload impacts because of complacency and related vigilance issues. Both ways, and everything in between, the consequences of this behavior will have a dramatic effect on safety.

All in all, we must also understand graceful degradation of system performance as well as the primary concerns with consequences to human interaction (primary consequences) and thus the early emphasis on failed and degraded modes analyses. How the system may degrade or fail must be understood with respect to the functional and safe use of the system. The safety case analyses again appears at this stage to help define and quantify.