

HUMAN FACTORS FAILURE MODES AND EFFECTS ANALYSIS (HF-FMEA) TOOL FOR PRE- AND POST-MISHAP INVESTIGATION

David M.A. Hollaway¹ and Christopher M. Pohlen²

¹Senior Aviation Safety Analyst, Black Swan SRC, LLC, dmah@blackswansrc.com

²Human Systems Integration, Black Swan SRC, LLC, cmp@blackswansrc.com

ABSTRACT

This paper presents the applicability of the HF-FMEA in aircraft accident investigation, the steps required to conduct an HF-FMEA using the SHEL Model as a starting point, identification of key failure modes and single-point weaknesses using guidewords, use of a severity and probability scoring matrix, performance-shaping factors, and an example of an HF-FMEA in an approach and landing accident. A Failure Modes and Effects Analysis (FMEA) is a systems safety engineering methodology for proactively assessing the vulnerabilities in a system before latent hazards may cause a mishap. In an aircraft (or any other) mishap, the HF-FMEA may be used as a forensic tool to identify where potential human errors may have occurred. Isolation of potential crew or human operator errors can illuminate causal factors which lead to the mishap. In the aftermath of an accident or near miss, an HF-FMEA may be applied to uncover deeper general system weaknesses that go beyond key failure modes that led directly to the mishap. An HF-FMEA can highlight other parallel and surrounding risks and causal factors that may not be discovered using a forced factor exclusion method such as root cause analysis (RCA) only.

Introduction

Mica Endsley states that, traditionally, aviation systems have been designed and developed from a technology-centered perspective. Engineers developed flight control systems to perform each function of the aircraft and provided a display for each system that informed the flight crew about the systems status. These displays (colloquially known as steam gauges) grew exponentially until they were replaced by digital electronic multifunction displays commonly referred to as “glass cockpits.” While this decreased the number of physical displays, the flight crew is still tasked with navigating display pages and displayed information required to evaluate the performance of the system, or what Norman called the “Gulf of Evaluation”, increased exponentially. In the face of changing tasks and situations, the human operator is required to find, sort, integrate, and process the data to determine the information needed to move the aircraft from its current state to a goal state.

Unfortunately, human operators of complex, tightly coupled systems such as aircraft under instrument meteorological conditions, have information processing limitations. Pilots can only pay attention to a limited number of items at any one time (typically six to ten) referred to as the span of control. The display of data required to perform a task is often scattered between displays, requiring a considerable amount of cognitive resources which leads to mistakes

(planning failures) or execution errors (slips and lapses). The more this cognitive workload increases, the more likely an error may be made by the flight crew. Human error is a causal factor in aircraft mishaps between 60 and 85 percent of the time.

One excellent tool for discovering the potential for human error in the operation of a complex system is the Human Factors Failure Modes and Effects Analysis (HF-FMEA). The HF-FMEA may be used to assess a particular human-machine interface (HMI) or task sequences for latent, error provocative design, or to elucidate potential human errors which may have been causal factors in a mishap. Identification of key failure modes and single point weaknesses in aircraft systems is an extremely important tool in mishap reduction efforts.

Human Factors Failure Modes and Effects Analysis (HF-FMEA)

Description of the Methodology

Failure Modes and Effects Analysis (FMEA) is a systems safety engineering methodology for proactively assessing the vulnerabilities in a system before active and latent hazards may cause a mishap. The Human Factors Failure Modes and Effects Analysis (HF-FMEA) methodology is carried out by a multidisciplinary team to proactively or retroactively analyze a human system interaction to discover active or latent potential error provocative hazards. The HF-FMEA is based on the philosophy that human errors can be controlled by managing the performance-shaping factors effecting human performance, erecting barriers to prevent human errors, adding controls to detect and correct human error before it leads to an undesirable outcome, and building error resistant and error tolerant systems. This methodology analyzes tasks within an evolution, process, or procedure to identify human errors that may lead to a mishap, the factor that make the system error provocative, the Worst-Case effects on the system, and provides containment and corrective actions to eliminate or mitigate the human error. The HF-FMEA considers:

- What human errors (guide words) could be committed, which is the failure mode;
- What are the consequential impacts if the human errors are committed, which is the failure effects;
- What is the probability that the human error will be committed, how severe are the consequential impacts to the system, and how detectable is the error if it is committed;
- What are the performance-shaping factors that cause the error to be committed; and
- What are the mitigation strategies to eliminate or mitigate the error or its consequential impacts?

The HF-FMEA improves on the traditional process-driven FMEA methodology by incorporating a range of human factors methods during the analysis to:

- Enable identification of failure modes from a human factors perspective;

- Account for human operator strengths and limitations when rating and prioritizing active and latent error opportunities;
- Identify causal factors from a human factors perspective, as opposed to hardware and software failure causes; and
- Identify human factors informed containment and corrective actions and set expectations about how much risk is likely to be mitigated given the proposed mitigation strategies.

The HF-FMEA combines the methodologies of a Process FMEA (PFMEA) and a Hazard and Operability (HAZOP) analysis with the incorporation of human factors. HAZOP is a standard methodology for preliminary safety assessment for new or modified products and is widely used in the process industries and others in detecting potential hazards and operational difficulties in a system. HAZOP is also used to analyze operating procedures to identify latent human errors that may exist in a task. The basic idea of a HAZOP is that any deviation from the procedure or operating conditions may cause a mishap due to human error.

The strength of a HAZOP is identification of failure modes (errors) caused by human operators. By dividing a complex task or scenario into smaller and more manageable nodes for study, and the systematic identification of process parameter deviations from goal states, provides thorough identification of human operational failure modes. However, a typical HAZOP is not strong in analyzing the effects and relative effectiveness of identified corrective actions and mitigation strategies. On the other hand, the PFMEA contains a thorough, semi-quantitative evaluation of the consequential impacts of failure modes. By analyzing and scoring based on the probability and severity attributes, the failure mechanism can be understood, and more importantly, the efficacy of mitigation strategies to prevent human error may be determined. Conversely, PFMEA is relatively weak in failure mode identification, as it does not provide a systematic method of evaluating human operational deviations due to error. Combination of the HAZOP and PFMEA methodologies gives rise to the HF-PFMEA; the combination of both methodologies provides a robust method for identification and mitigation of potential human errors in a system.

Since a flight crew can only interact with the aircraft through displays and controls, the HF-FMEA will identify potential human errors induced by the human-machine interface (HMI).

Description of the HF-FMEA Procedure

The following presents the procedural guidelines for performing an HF-FMEA. The HF-FMEA process is comprised of 10 steps outlined in Figure 1. Each step is described in detail below.

Step 1 – Select and Define the Scope of the Process

The most critical step of the HF-FMEA is to select a process to analyze. A process is a series of tasks undertaken to achieve a goal state, bounded by a defined beginning and end. A process

may be focused on an aircraft system functionality or may define a series of workflow tasks required to reach a goal state.

When choosing a process, it should be sufficiently high-risk and error provocative to justify the effort involved in conducting the analysis; processes involving low levels of automation and high levels of human supervisory control such as a Category II or III instrument approach should be analyzed. Comparing the residual risk associated with different procedures or automation options for implementation or analyzing the general human error risks related critical tasks usually justify the HF-FMEA.

To support a successful HF-FMEA, the process scope included for analysis must be clearly defined. To do this, the starting and ending points of the process must be established, as these are the boundaries that will define the scope of the analysis.

A well-defined and manageable process scope is essential to prevent the required resources and scope from escalating out of control. When defining a process scope for analysis, always lean towards too narrow a process, rather than a process that may be too broad, as there is almost no process that is too narrow for the application of an HF-FMEA.

To help define the process scope for an HF-FMEA, consider the proposed process on several levels and explicitly define what will be included and excluded. Categories of information to include or exclude depend on the process under consideration, but the SHEL Model may be useful (Figure 2).

The SHEL Model is a conceptual tool used to analyze the interaction of multiple system components. The model is named from the initial letters of its components, Software, Hardware, Environment, and Liveware (SHEL). The model diagram uses blocks to represent the different components of a system interacting with the human operator and teams of human operators (human factors). This building block diagram does not cover interfaces which are outside of human factors, i.e., hardware-hardware, hardware-environment, software-hardware, and is only intended as a basic memory aid for considering flight crew interactions for the HF-FMEA.

- **(S) Software** – for the purposes of the HF-FMEA, software does not refer to the computer code for the operation of automatic systems such as Mach trim, yaw dampening, or autoflight operations, but the regulatory flight rules, standard operating procedures (SOP), memory aid checklists, quick reference handbooks (QRH), ACARS or EICAS messages, Caution and Warning (C&W) messages and tones, etc.
- **(H) Hardware** – the displays and controls with which the flight crew interact with the aircraft systems.
- **(E) Environment** – the situation in which the L-H-S system must function, including levels of automation and human supervisory control (technical environment), system requirements, and the internal and external physical environment.

- **(L) Liveware** – the flight crew interacting with each other, the cabin crew, air traffic control, and/or company operations (dispatch) on the ground. This includes interactions within a group (flight crew and cabin crew) and between groups (flight crew and ATC or company dispatch).

Table 1 provides an example of configuring a transport category airplane for landing and some of the variables that might be considered for inclusion or exclusion when defining the scope for the process of landing.

Step 2 – Assemble the Investigatory Team

Once the process, starting and ending points, and inclusion and exclusion criteria have been defined, a team must be assembled to conduct the analysis. Like all mishap investigations, teams should be multidisciplinary, representing a range of knowledge, experiences, backgrounds, and perspectives. The personnel chosen to participate in the HF-FMEA will depend on the process and scope being analyzed. As much as possible, team members should be chosen who are knowledgeable about the defined process scope, and who will think critically about the process from the human-centered design process and human operator perspective, provide input, feedback, guidance, and buy-in at various stages of the HF-FMEA analysis.

Individual team members may fulfill several different roles to ensure a successful analysis. Each HF-FMEA team should include individual members who can serve as subject matter or process experts, process reviewers, and senior advisors. Additionally, some of these same team members may take on the roles of team leader or facilitator, scribe, and human factors subject matter experts (SME).

- **Process SME** – personnel who have a detailed understanding of any technologies, processes, and environments being studied. These team members will be central to mapping the process being analyzed, identifying potential risks, assessing and rating risks, and providing input when proposing and identifying the impact of mitigating strategies. Subject matter or process experts include, but are not limited to, airframe, powerplant, or avionics subsystem design engineers, autoflight system and flight software design engineers, vendor systems engineers, etc.
- **Process Reviewers** – personnel who are less familiar with the process being analyzed, but who have experience and knowledge in a related field. Process reviewers are important for providing a critical review of practices and standards that are accepted by the aviation community. Team members fulfilling this role are more likely to identify vulnerabilities that are not detected by process experts. Process reviewers generally are frontline human operators (flight or cabin crew or maintenance personnel).
- **Senior Advisors** – generally the operations and maintenance personnel at the certificate management level (e.g., Director of Operations, Director of Maintenance, Chief Pilot, Director of Training, Director of Safety, or union representative), or senior staff members, who can provide a broad organizational and operational perspective to the

team. These individuals help to facilitate access to the resources, such as personnel and logistical support, which are required to conduct an effective HF-FMEA. Senior advisors also play a key role in achieving buy-in from areas in the program organization where changes will be implemented based on the mitigating strategies identified in the analysis, and for facilitating any scope, requirements, or technical changes.

- **Team Leader or Facilitator** – the team member responsible for keeping the discussion during meetings moving and on target. The team leader should encourage participation from team members who may be more reluctant to express their ideas. The team leader should be confident, good at managing people, group dynamics, and able to facilitate group consensus building.
- **Scribe** – person responsible for capturing the discussion and decisions made at each analysis meeting and circulating meeting minutes to the entire team.
- **Human Factors SME** – person or personnel who have detailed aviation human factors training and certification. The human factors perspective is extremely important because human strengths and limitations are considered when identifying and rating failure modes, and when identifying causes and recommendations. Applying human factors expertise is essential for each of these HF-FMEA steps.

HF-FMEA teams generally range in size from about three to eight personnel, but the exact number will depend on the process scope and how many stakeholders are affected by the process being analyzed. When too few team members are included in an HF-FMEA, the analysis will be less robust, with the possibility of being incomplete, if relevant perspectives are not included. Conversely, when too many team members are included, it can be increasingly difficult to schedule meetings, coordinate and compile team member's process work, and reach consensus.

An effective balance can be reached by tending towards a larger team, but then breaking that team into a work team and an advisory team. The work team should consist of two or three people who are responsible for conducting the detailed analysis and reporting back to the larger team. The work team should meet several times and dedicate their time to leading the hands-on work including creating diagrams, formulating the analysis, and producing reports. The advisory team, who make up the balance of the entire HF-FMEA team, is responsible for reviewing the analysis of the work team and providing guidance and resources as required during several key meetings. Key meetings take place throughout a HF-FMEA to ensure the perspectives, experience and ideas of all stakeholders are included in the analysis. The first meeting (kick-off) should be conducted once the team is selected and a process is proposed.

Step 3 – Identify Controls and Displays

Identify the controls and displays that are to be used by the flight crew to perform the tasks to accomplish the goal state.

Step 4 – Identify Required Actions by the Flight Crew

Identify the input actions required to be executed by the flight crew to accomplish the goal state.

Step 5 – Identify Required Feedback to the Flight Crew

Identify the salient feedback to the flight crew which are outputs from the aircraft's systems in response to the crew's inputs in Step 4.

Step 6 – Perform a Hierarchical Task Analysis (HTA)

Once the team has been assembled and consensus has been reached on the process scope (i.e., start and end points, inclusion and exclusion criteria), and the human operator's inputs and outputs to the human operator as feedback, the process must be documented. Documenting the process means creating a graphical representation of the steps and sub-steps required to complete the chosen process scope. Generally, this is accomplished through the creation of a Hierarchical Task Analysis (HTA); the HTA is the most commonly used human factors method and is typically used a start point or basis of any human factors analysis.

The HTA involves describing the activity or process under analysis in terms of a hierarchy of goals, sub-goals, operations, and plans. The result is an exhaustive description of task activity. Most human factors analyses methods require an initial HTA of the task under analysis as an input. The HTA may be started from scratch or may use a checklist or other memory aid as an initial input. The HTA should be performed by the HF-FMEA work group. A flowchart for conducting an HTA is presented in Figure 3 below.

There are seven steps to performing an HTA which are described here.

HTA Step 1 – Define Task Under Analysis

The first step in conducting an HTA is to clearly define or bound the task(s) under analysis. This step is the same as Step 1 for the HF-FMEA.

HTA Step 2 – Data Collection

Once the task under analysis is clearly defined, specific data regarding the task should be collected. The data collected during this process is used to inform the development of the HTA. Data regarding the task steps involved, the levels of automation and interfaced used, human computer interactions, decision-making, consequence guidance, caution and warnings, and task constraints should be collected. There are several ways to collect this data, including observations of aircraft system functionality, interviews with Process SMEs, questionnaires, and functionality demonstrations in a Level C or D simulator. The methods used for data collection are dependent upon the analysis effort and the various constraints imposed, such as time, logistical, or flight crew personnel constraints. Once enough data regarding the task under analysis is collected, the development of the HTA should begin.

HTA Step 3 – Determine the Overall Goal, Conditions, and Success Criteria of the Task

The overall goal of the task under analysis must first be specified at the top of the hierarchy. The task must be clearly defined and rationally bounded. An example task of “Configure Aircraft for Landing” is presented. It is often helpful to use the SMART acronym when defining the task:

- **Specific** – is the task well-defined, clear, concise, and unambiguous?
- **Measurable** – what specific criteria will be used to determine if (or when) the goal state of the task is achieved.
- **Achievable** – is the goal state achievable given the conditions under which the task is to be performed, the resources and time available, the time required, and the success criteria defined?
- **Relevant** – are the actions required to achieve the goal state and only those actions?
- **Time-Bound** – is there a clearly defined timeline with objective start and stop points based on time available and time required to achieve the goal state?

HTA Step 4 – Determine Sub-Task Goals

Once the overall task goal has been specified, the next step is to break this overall goal down into meaningful sub-goals (usually four or eight but this number is not rigid), which together form the activities required to achieve the overall goal.

HTA Step 5 – Subgoal Decomposition

Next, the subgoals identified in HTA Step 4 should be decomposed into further sub-goals and operations.

This decomposition should continue until an appropriate level of operational detail is reached. The bottom level of any branch in an HTA should always be an operation; while everything above an operation specifies goals, operations specify what action or actions the human operator must take to achieve the goal state.

HTA Step 6 – Plan Analysis

Once all sub-goals and operations have been fully described, the plans required to achieve the goal are constructed. A simple plan would say Do 1, then 2, then 3. Once the plan is completed, the human operator returns to the superordinate level. Plans do not have to be linear or temporally or spatially related, such as Do 1, or 2 and 3. The different types of plans used in an HTA are presented in Table 2. The output of the HTA may either be a tree diagram (Figure 4) or a table (Table 3).

HTA Step 7 – HTA Exit

There are no success criteria for the HTA but is an initial input to the HF-FMEA. The HTA is a living methodology in that it is continuously evaluated for accuracy and relevance

throughout the HF-FMEA process and is updated to reflect changes in tasks driven by output from the HF-FMEA.

Step 7 – Identify Failure Modes and Effects Using Guidewords

Identify potential human error failure modes and effects using the 12 guide words. The guide words provide causes of deviation from a required action or task step due to a human error (slip, lapse, or mistake) which may be an error of omission (omit/skip, less than, or part of) or commission (more than, less than, too early, too fast, too late, too slow, as well as, other than, reverse, or out of sequence); errors may be intentional or unintentional acts by the human operator.

1. Omit/Skip – the specified action or step is not performed as required.
2. More Than – a quantitative increase in the specified action or step over that required.
3. Less Than - a quantitative decrease in the specified action or step over that required.
4. Sooner Than – the specified action or step is quantitatively correct but is performed before it is required.
5. Faster Than – the specified action or step is quantitatively correct but is performed more rapidly than required.
6. Later Than – the specified action or step is quantitatively correct but is performed after it is required.
7. Slower Than – the specified action or step is quantitatively correct but is performed more slowly than required.
8. As Well As – the specified action or step is quantitatively and temporally correct, but some unrequired additional action is performed.
9. Part Of – the specified action or step is not completely performed (partial omit/skip).
10. Reverse – the specified action or operation is performed, but the opposite of the design goal state occurs (emergent behavior).
11. Other Than – an incorrect and complete substitution for the specified action or step is performed.
12. Out of Sequence – the specified action or step is both quantitatively and temporally performed, but not in the required sequence.

Deviation is the combination of a guide word and a required action or task step. The combination of a guide word or required action or task step should be meaningful and possible. Deviations which not credible because they cannot occur or are duplicative to another guide word should be documented as considered but otherwise omitted to improve the efficiency of

the analysis. For example, OMIT plus LANDING GEAR LEVER DOWN during the landing phase of flight is credible. Conversely, PART OF plus FLAP RETRACTION during the climb out phase of flight is duplicative to LESS THAN and TOO LATE plus FLAP RETRACTION; since the errors are the same, only one should be documented. Moreover, TOO EARLY plus FLAP RETRACTION is credible but duplicative to MORE THAN. However, TOO FAST plus FLAP RETRACTION during the climb out phase of flight is not credible since the human operator does not have control over the flap retraction speed, only the degree of retraction. The main point is to choose the guide word that has the greater impact on the system in terms of quantitative or temporal consequential impacts.

Note that the failure cause (slip, lapse or mistake) due to a performance shaping factor such as fatigue, circadian dysrhythmia, medical illness, hypoxia, loss of situational awareness, complacency, stress, task saturation, channelized attention, physical limitation, inadequate experience for complexity of situation, insufficient reaction time, or physical or technological environment, are not considered at this step. Only that an error of intentional or unintentional commission or omission from one of the 12 failure modes WILL occur at some time in the aircraft's operational life cycle is considered.

For each failure mode, the HF-FMEA describes the worst-case consequential effect. The failure mode consequential effects are described at the following indenture levels:

- Immediate Effect – failure effect on aircraft system, subsystem, component, or device and its functional output.
- Systemic Effect – propagation of the failure effect on other systems or aircraft performance effect (flight path, altitude, terrain clearance, etc.).

To identify the possible consequential effects of each failure mode, the team should think through what could possibly happened if the human error occurs. When several different consequential effects are possible, the worst-case consequential effect is considered to the exclusion of the others.

The following list is adapted from design failure modes and effects analysis (DFMEA). The list of consequential effects may be used in the HF-FMEA.

- No Output
- Erroneous Output
- Fail to Open/Extend
- Fail to Close/Retract
- Fail to Start/Stop
- Fail to Switch/Transfer
- Loss of Output
- Failure to Perform Function
- Failure to Operate at Prescribed Time
- Output Too Early/Too Late

- Output Excessive/Inadequate
- Fail to Remain Open/Extended
- Fail to Remain Closed/Retracted
- Fail to Engage/Disengage
- Inadvertent Open/Close
- Loss of Control
- Erroneous Indication
- Erratic Operation
- Computer Halt Interrupt
- Induce Wait State, Dead State, or Orphan State
- Measurement Anomaly
- No Effect
- Not Specified/Unknown

Step 8 – Rate Failure Modes and Effects for Severity and Probability

Step 7 will generate a significant list of possible human error failure modes and resultant effects. However, every failure mode and effect cannot be mitigated; therefore, the team must concentrate on those failure modes and effects which present the highest risk to the flight crew, aircraft, or mission. To identify those human error failure modes and effects which may have high risk consequential impacts, and thus require the most mitigation effort, each failure mode and effect is rated using risk-scoring matrices. Risk-scoring matrices are rubrics that support the assignment of risk scores to each failure mode effect. In the HF-FMEA framework, two matrices are used to support the identification of key failure modes: a severity-scoring matrix and a probability-scoring matrix. The probability-scoring matrix is supported by a task hazard assessment matrix.

The severity-scoring matrix is presented in Table 4. The criticality category for a failure mode is based on the worst-case potential effect, assuming a loss of all redundancy, error resistance, and error tolerance controls. This includes possible catastrophic effects as well as the effects of hardware functions.

The probability-scoring matrix is presented in Table 5. Probability is based on a subjective assessment of the team based on interaction with the system as to how often the human error may occur.

In estimating the probability of the error occurrence, a task hazard assessment is performed on the top-level task using the performance-shaping factors (PSF) criteria in Table 6. The PSF in Table 6 are the causal factors which may induce a human error during the performance of the task under analysis.

The cumulative score from the assessment is used to determine the probability of a human operator error in Table 5 probability-scoring matrix above.

Step 9 – Determine Key Failure Modes (KFM)

Once the severity and probability of each failure mode and effect has been rated using the appropriate matrices, a series of three tests are applied to determine Key Failure Modes (KFM). The three tests are the Severity Test, the Hazard Score Test, and the Single Point Weakness (SPW) Test. The tests should be applied according to Figure 5.

Test 1 – Severity Score

Any human error failure mode and effect having a severity score ≥ 3 is automatically classified as a KFM and requires a mitigation strategy.

Test 2 – Hazard Score

The hazard score for each human error failure mode and effect is determined by multiplying the severity and probability scores. If the hazard score is ≥ 8 , it is evaluated for control and detectability to determine if the failure mode is a KFM.

The first consideration is to ask if the failure mode is effectively controlled. An effectively controlled failure mode has an intervention that is inherent to the system that eliminates or substantially reduces the likelihood of a fault, failure, or off-nominal condition or event due to human error (i.e., the system is error resistant and error tolerant). The control to prevent the human error failure must be provided by a software function and not by an administrative control. The method of control must be documented in the HF-FMEA.

If the failure mode is effectively controlled by the error resistance and error tolerance of the system, it is excluded as a KFM.

The second consideration is to ask if the failure mode is obviously detectable. A detectable failure mode is an obvious hazard that is likely to be easily detected by the human operator and, because of its detectability, does not require an effective control measure. To determine if the failure mode is detectable, the following statements are considered. If any the statements are TRUE, the failure mode is not sufficiently detectable and is classified as a KFM:

- There is no possible way to detect the error such as through salient feedback, consequence guidance, or generation of a caution or warning alert.
- The error can only be detected through a visual inspection and is not feasible or readily accomplished so the error remains latent.
- The error can be detected through visual inspection, but there the index of suspicion required to prompt the human operator to make the inspection is so low that the detection of the error is left to chance.
- There is a process for error cross-checking or detection, but the process relies on human operator vigilance or is applied only to a statistical data sample.

If a human error failure mode has a hazard score ≥ 8 and is neither controlled nor detectable are classified as KFM and will require a mitigation strategy. If the human error failure mode has a

hazard score of ≥ 8 and is either effectively controlled, detectable, or both, it is documented but does not require a mitigation strategy.

If a human error failure mode has a hazard score < 8 , it is evaluated for cause of a single point fault, failure, or off-nominal condition or event that may have a catastrophic or severe effect. If the failure mode effect may cause a catastrophic or severe fault, failure, or off-nominal condition or event, Test 3 is applied. If the failure mode effect will not cause a catastrophic or severe fault, failure, or off-nominal condition or event, is automatically excluded as a KFM.

Test 3 Single Point Weakness (SPW)

For those human error failure modes and effects that have a hazard score < 8 and are neither controlled nor detectable, the Single Point Weakness (SPW) test is applied. A SPW is any single human error that, if not effectively controlled or detected, may cause a catastrophic or severe fault, failure, or off-nominal condition or event.

If a human error failure mode with a hazard score < 8 is identified as a SPW, the same two considerations for control and detectability in Test 2 are applied.

If the SPW is neither controlled nor detectable, it is classified as a KFM and requires a mitigation strategy. If the SPW is either effectively controlled, detectable, or both, it is documented but does not require a mitigation strategy.

Step 10 – Develop and Implement Mitigation Strategies or Identify Potential Causal Factors

The final step of the HF-FMEA is to develop and implement mitigating strategies that address the performance shaping factors (PSF) in Table 6 to reduce the probability and/or severity through control, or increase the detectability of a failure mode effect, using the hierarchy of effectiveness shown in Table 7.

If the HF-FMEA is used as a mishap investigation tool, all KFM and SPW identified should be considered potential causal factors in the conduct of a forced-factual root cause analysis.

Completion of the HF-FMEA

If the HF-FMEA is being used as a human error prevention design tool, the HF-FMEA is completed once mitigation strategies have been prioritized, a decision has been made about which solutions will be implemented, and a plan is developed to support the successful implementation each mitigation strategy. The plan for each strategy should outline (1) the disciplines or project teams responsible for implementing the strategy, (2) the outcome measures that will be used to assess the success criteria, (3) the anticipated timelines, and (4) a plan for proactively evaluating new failure modes that are likely to be associated with the system changes made through implementing the mitigating strategies.

A summary report should be prepared by the work team that outlines the HF-FMEA process, team members, key decisions, lessons learned, and progress implementing mitigating strategies

to date. This document should be circulated to the advisory team for review and approval before sharing more broadly with stakeholders.

If the HF-FMEA is being used as a mishap investigation tool, the HF-FMEA is completed when all KFMs and/or SPW have been identified and used as an input for a root cause analysis.

Success Criteria

The success criteria are met when all KFMs have been mitigated or, for any KFMs that cannot be successfully mitigated through engineering or administrative controls, the risk is accepted by the authority having jurisdiction over the aircraft certification or other major stakeholders such as the owner or operator.

Conclusions

HF-FMEA may be used as a forensic tool to identify where potential human errors may have occurred. Isolation of potential crew or human operator errors can illuminate causal factors which lead to the mishap. In the aftermath of an accident or near miss, an HF-FMEA may be applied to uncover deeper general system weaknesses that go beyond key failure modes that led directly to the mishap. An HF-FMEA can highlight other parallel and surrounding risks and causal factors that may not be discovered using a forced factor exclusion method such as root cause analysis (RCA) only.

The HF-FMEA is based on the philosophy that human errors can be controlled by managing the performance-shaping factors effecting human performance, erecting barriers to prevent human errors, adding controls to detect and correct human error before it leads to an undesirable outcome, and building error resistant and error tolerant systems.

Identification of key failure modes and single point weaknesses in aircraft systems is an extremely important tool in mishap reduction and investigatory efforts.

References

Borghini, G., Arico, P., Di Flumeri, G. and Babiloni, F. (2017). *Industrial Neuroscience in Aviation: Evaluation of Mental States in Aviation Personnel*. New York: Springer Publishing Company.

Campbell, R.D. and Bagshaw, M. (2002). *Human Performance and Limitations in Aviation*. Ames, IA: Blackwell (Iowa State University Press).

Department of Defense (DoD) (1984). *MIL-STD-1629A Procedures for Performing a Failure Modes and Effects Analysis (FMEA)*. Washington, DC: Author.

Dyadem Engineering Corporation (2004). *Guidelines for Failure Mode and Effects Analysis (FMEA) for Automotive, Aerospace, and General Manufacturing Industries* (1st Ed.). Ontario, Canada: Dyadem Press (Author).

- Endsley, M.R. and Jones, D.G. (2012). *Designing for Situation Awareness: An Approach to User-Centered Design* (2d Ed.). Boca Raton, FL: CRC Press.
- Hawkings, F.H. (1987). *Human Factors in Flight* (2d ed). (Orlady, H.W., Ed.). Burlington, VT: Ashgate Publishing.
- Johnston, N., McDonald, N., and Fuller, R. *Aviation Psychology in Practice*. Brookfield, VT: Ashgate Publishing.
- Kirwan, B. and Ainsworth, L. K. (Eds). (1992). *A Guide to Task Analysis*. Boca Raton, FL: CRC Press.
- Norman, D.A. (2013). *The Design of Everyday Things (Rev. Ed.)*. New York: Basic Books, Inc.
- O'Hare, D. (2006). *Cognitive Functions and Performance Shaping Factors in Aviation Accidents and Incidents*. *International Journal of Aviation Psychology*, 16(2), 145-146.
- Perrow, C.B. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, Inc.
- Proctor, R.W. and Van Zandt, T. (2018a). *Reliability and Human Error in Systems*. In Proctor, R.W. and Van Zandt, T. *Human Factors in Simple and Complex Systems (3d Ed.)*. Boca Raton, FL: CRC Press.
- Proctor, R.W. and Van Zandt, T. (2018b). *Human Information Processing*. In Proctor, R.W. and Van Zandt, T. *Human Factors in Simple and Complex Systems (3d Ed.)*. Boca Raton, FL: CRC Press.
- Reason, J. (1990). *Human Error*. Cambridge, UK: Cambridge University Press.
- Reason, J. (1997). *Managing the Risk of Organizational Accidents*. Burlington, VT: Ashgate Publishing.
- Rong, M., Zhao, T., and Yu, Y. (2008). *Advanced Human Factors Process Failure Modes and Effects Analysis*. Annual Reliability and Maintainability Symposium, Las Vegas, NV, USA, 2008, pp. 365-370, doi: 10.1109/RAMS.2008.4925823.
- Stamatis, D.H. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution (2d Ed.)*. Milwaukee, WI: American Society for Quality (ASQ).
- Stanton, N.A., Salmon, P.M., Rafferty, L.A., Walker, G.H., Baber, C., and Jenkins, D.P. (2013). *Human Factors Methods: A Practical Guide for Engineering and Design (2d Ed.)*. Burlington, VT: Ashgate Publishing.
- Stanton, N.A. and Barber, C. (2005). *Task Analysis for Error Identification*. In N.A. Stanton, et al (Eds.), in *Handbook of Human Factors and Ergonomics Methods*. Boca Raton, FL: CRC Press.

Strauch, B. (2004). *Investigating Human Error: Incidents, Accidents and Complex Systems*. Burlington, VT: Ashgate Publishing.

Tsang, P.S., Vidulich, M.A., and Kantowitz, B.H. (Eds.) (2002). *Principles and Practice of Aviation Psychology*. Burlington, VT: CRC Press.

Weigmann, D.A. and Shappell, S.A. (2003). *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*. Burlington, VT: Ashgate Publishing.

Wood, R. and Sweginnis, R. (2006). *Aircraft Accident Investigation* (2d ed.) Casper, WY: Endeavor Books.

TABLE 1
PROCESS: Configure A/C for Landing when In-Range

SHEL ELEMENT/TASK STEPS	INCLUDED	EXCLUDED
(S) Software		
• Instrument Approach Procedure (IAP)		✓
• A/C Checklist and Quick Reference Handbook (QRH)	✓	
• FAR Part 91 General Operating and Flight Rules		✓
• EICAS Messages		✓
• ACARS Messages		✓
• ATIS Messages	✓	
(H) Hardware		
• Primary Flight Controls		✓
• Secondary Flight Controls	✓	
• Primary Flight Displays	✓	
• Multifunction Flight Displays	✓	
• FMS Control Display Unit (CDU)	✓	
• Master Control Panel (MCP)	✓	
(E) Environment		
• Level of Automation (Raw Data/HDG/Coupled/CAT II)	✓	
• Physical (Convective Turbulence/Day/Night)	✓	
• Runway (Precision/Non-Precision/Approach Lighting System)		✓
• FAR 91 Approach Requirements		✓
• ATC Services (Radar/Non-Radar)		✓
(L) Liveware		
• Flightcrew Interaction (CRM)	✓	
• Flightcrew/ATC Interaction		✓
• Flightcrew/Company Dispatcher Interaction		✓
Task Steps		
• Receive ATIS/Approach Clearance		✓
• Set Approach in FMS		✓
• Set AFDS to CMD FMS		✓
• Initiate Descent from Initial Approach Fix (IAF)	✓	
• Set Aircraft Speed to 190 KIAS	✓	
• Set TEF to FLAPS 1	✓	
• Reduce Airspeed to 150 KIAS	✓	
• Set TEF to FLAPS 5	✓	
• Set TEF to FLAPS 15	✓	
• Reduce Airspeed to VREF +10 KIAS	✓	
• Extend Landing Gear	✓	
• Set TEF to FLAPS 25	✓	

TABLE 2
EXAMPLE OF HTA PLANS

PLAN	EXAMPLE
Sequential (Condition Precedent)	Do 1 then 2 then 3
Non-Sequential (No Conditions Precedent)	Do 1, 2, and 3 in any order
Simultaneous or Parallel	Do 1, then 2 and 3 at the same time
Branching	Do 1, if X present, then do 2 and 3; if X is absent, EXIT
Cyclical	Do 1 then 2 then 3 and repeat until X is achieved
Selection	Do 1 then 2 or 3

TABLE 3
HTA for CONFIGURE AIRCRAFT FOR LANDING

Autoflight Assumption: AFDS CMD Mode ALT HOLD, V/S, ALT AQD, or LVL CHG; A/T Switch ARM; N1 Mode Disengaged; MCP SPD in A/T Mode in pitch (A/T does not set thrust above displayed N1 limit but A/T may exceed N1 value manually set by N1 manual set knob), A/C at or approaching IAF and Altitude.

3. Configure Aircraft for Landing
Plan 3: Do 3.1 through 3.10 sequentially

3.1 Check Distance to Runway using EADI DME

3.2 Reduce Airspeed to 190 KIAS
Plan 3.2: Do 3.2.1 to 3.2.4 sequentially

- 3.2.1 Set MCP IAS/Mach Speed Control to IAS with Changeover (C/O) switch
- 3.2.2 Check current airspeed on PFD airspeed setting bug
- 3.2.3 Set airspeed to 190 KIAS in IAS/Mach display window using airspeed knob on MCP
- 3.2.4 Check airspeed trend down on PFD airspeed tape indicator

3.3 Set Trailing-Edge Flaps (TEF) and Leading-Edge Devices (LED) to FLAPS 1
Plan 3.3: Do 3.3.1 to 3.3.4 sequentially

- 3.3.1 Check current airspeed on PFD airspeed indicator for flap overspeed precaution
- 3.3.2 Check current flap position agreement with flap lever and flap position indicator
- 3.3.3 Set flap lever to FLAP 1 position (LED will automatically extend with TEF at FLAPS 1)
- 3.3.4 Check flap position agreement with flap lever and flap position indicator

3.4 Reduce Airspeed to 150 KIAS
Plan 3.4: Do 3.4.1 to 3.4.3 sequentially

- 3.4.1 Check current airspeed on PFD airspeed setting bug
- 3.4.2 Set airspeed to 150 KIAS in IAS/Mach display window using airspeed knob on MCP
- 3.4.3 Check airspeed trend down on PFD airspeed tape indicator

3.5 Set Trailing-Edge Flaps (TEF) to FLAPS 5
Plan 3.5: Do 3.5.1 to 3.5.4 sequentially

- 3.5.1 Check current airspeed on PFD airspeed indicator for flap overspeed precaution
- 3.5.2 Check current flap position agreement with flap lever and flap position indicator
- 3.5.3 Set flap lever to FLAP 5 position
- 3.5.4 Check flap position agreement with flap lever and flap position indicator

3.6 Reduce Airspeed to 140 KIAS
Plan 3.6: Do 3.6.1 to 3.6.3 sequentially

- 3.6.1 Check current airspeed on PFD airspeed setting bug
- 3.6.2 Set airspeed to 140 KIAS in IAS/Mach display window using airspeed knob on MCP
- 3.6.3 Check airspeed trend down on PFD airspeed tape indicator

3.7 Set Trailing-Edge Flaps (TEF) to FLAPS 15
Plan 3.7: Do 3.7.1 to 3.7.4 sequentially

- 3.7.1 Check current airspeed on PFD airspeed indicator for flap overspeed precaution
- 3.7.2 Check current flap position agreement with flap lever and flap position indicator
- 3.7.3 Set flap lever to FLAP 15 position

	3.7.4 Check flap position agreement with flap lever and flap position indicator
3.8	Extend Landing Gear Plan 3.8: Do 3.8.1 then 3.8.2
	3.8.1 Move landing gear handle from OFF to DOWN position 3.8.2 Check landing gear position lights (verify three green)
3.9	Reduce Airspeed to VREF + 10 KIAS Plan 3.9: Do 3.9.1 to 3.9.4 sequentially
	3.9.1 Check current airspeed on PFD airspeed setting bug 3.9.2 Obtain VREF airspeed from FMS CDU landing page 3.9.3 Set airspeed to VREF +10 KIAS in IAS/Mach display window using airspeed knob on MCP 3.6.4 Check airspeed trend down on PFD airspeed tape indicator
3.10	Set Trailing-Edge Flaps (TEF) to FLAPS 25 Plan 3.10: Do 3.10.1 to 3.10.4 sequentially
	3.10.1 Check current airspeed on PFD airspeed indicator for flap overspeed precaution 3.10.2 Check current flap position agreement with flap lever and flap position indicator 3.10.3 Set flap lever to FLAP 15 position 3.10.4 Check flap position agreement with flap lever and flap position indicator
EXIT	

**TABLE 4
SEVERITY-SCORING MATRIX**

SEVERITY	DESCRIPTION	DEFINITION
4	CRITICAL	Single consequential effect which could result in a catastrophic event (loss of aircraft) or fatal or serious injury to flight crew or passengers.
3	SEVERE	Single consequential effect that could result in serious injury to flight crew or passengers, substantial damage to the aircraft or hull loss only.
2	MODERATE	Single consequential effect that could result in minor injury to flight crew or passengers, significant degradation of aircraft or system performance, or loss of critical redundancy.
1	MINOR	Single consequential effect that could result in a minor degradation of aircraft or system performance or loss of non-critical redundancy.

**TABLE 5
PROBABILITY-SCORING MATRIX**

PROBABILITY	DESCRIPTION	DEFINITION
4	FREQUENT	Error may occur multiple times during a flight or more than 5- yr ⁻¹ OR task hazard analysis cumulative score of <39.
3	PROBABLE	Error may occur more than once during a flight or may happen more than 2-yr ⁻¹ but less than 5- yr ⁻¹ OR task hazard analysis cumulative score of 30 to 39.
2	OCCASIONAL	Error may occur once during a flight or may happen more than 1-yr ⁻¹ but less than 2- yr ⁻¹ OR task hazard analysis cumulative score of 20 to 29
1	REMOTE	Error unlikely to occur during a flight or greater than 1-yr ⁻¹ OR task hazard analysis cumulative score <19.

**TABLE 6
TASK HAZARD ASSESSMENT
PERFORMANCE SHAPING FACTOR CRITERIA**

PSF		PURPOSE
FLIGHT CREW		Determine whether the task is executed by the flight crew, or between the flight crew and ATC or dispatch.
RANK	ASSESSMENT	CRITERIA
3	Flight Crew and ATC and Dispatch	Task can only be completed through coordination between the flight crew, ATC, and company dispatch.
2	Flight Crew and ATC	Task can only be completed through coordination between the flight crew and ATC.
1	Flight Crew	Task can be completed by the flight crew without external coordination.
PSF		PURPOSE
SITUATIONAL AWARENESS (SA)		Determine which entity will have the best information for making decisions and conducting operations when beginning the task.
RANK	ASSESSMENT	CRITERIA
4	Crew	Task requires SA that is only available to flight crew.
3	ATC	Task requires SA that is only available to an ATC controller and must be communicated to the flight crew.
2	Crew/ATC	Task requires SA that is available to any human operator but not automated systems.
1	Autoflight	Task requires autoflight capabilities.
PSF		PURPOSE
AVAILABLE REACTION TIME		Determine how much reaction time is available to the human operator before a worse-case consequential effect may occur.
RANK	ASSESSMENT	CRITERIA
4	Seconds	1 to 60 seconds.
3	Minutes	60 seconds to 10 minutes.
2	Hours	10 minutes to 1 hour.
1	End of Flight	1 hour to flight completion.
PSF		PURPOSE


TASK COMPLEXITY		Determine the level of difficulty of the task based on system knowledge requirements, knowledge-based decision-making requirements, and integration between additional systems.
RANK	ASSESSMENT	CRITERIA
3	High	High familiarity with system functionality required OR integration required with >2 additional systems. Task has >7 secondary tasks per instruction.
2	Medium	Moderate familiarity with system functionality required OR integration required between 1 or 2 additional systems. Task has between 4 and 7 secondary tasks per instruction.
1	Low	Minor familiarity with system functionality required OR no integration with additional systems required. Task has <3 secondary tasks per instruction.
PSF		PURPOSE
TASK DURATION		Determine duration of task based on number of procedural steps or time required to complete by a human operator.
RANK	ASSESSMENT	CRITERIA
3	High	More than 20 steps or more than 60 minutes.
2	Medium	Between 10 and 20 steps or between 20 and 60 minutes.
1	Low	Less than 10 steps or less than 20 minutes.
PSF		PURPOSE
TASK FREQUENCY		Determine how often the task is performed (recency).
RANK	ASSESSMENT	CRITERIA
4	Rarely	Task conducted in response to a fault, failure, or off-nominal condition or event (abnormal or emergency procedure).
3	Low	Task conducted monthly to quarterly or once per several flights.
2	Medium	Task conducted daily to weekly or once per flight.
1	High	Task conducted multiple times per day or per flight.
PSF		PURPOSE
TASK UNCERTAINTY		Determine the amount of uncertainty associated with task execution.
RANK	ASSESSMENT	CRITERIA
3	High	Contains 4 or more possible paths dependent on system data, decision-making or consequence guidance; OR 3 or more human operators involved; one of which is not a member of the same team.

2	Medium	Contains 2 or 3 possible paths dependent on system data, decision-making or consequence guidance; OR only 1 human operator involved; OR 2 human operators involved from different teams.
1	Low	No uncertainty with one possible path; OR 2 human operators from the same team involved using crew resource management (CRM) error prevention.
PSF		PURPOSE
OPERATOR FEEDBACK		Determine the required timeliness of operator feedback.
RANK	ASSESSMENT	CRITERIA
4	Immediate	Immediate feedback required after task execution (1 to 60 seconds).
3	Short	Feedback required within 60 seconds to 60 minutes.
2	Moderate	Feedback required in daily status report.
1	None	No feedback required.
PSF		PURPOSE
KNOWLEDGE AND TRAINING REQUIREMENTS		Determine the system knowledge and training requirements for human operators to maintain task proficiency.
RANK	ASSESSMENT	CRITERIA
3	High	Deep system knowledge training over years; refresher training required prior to every execution or less than monthly.
2	Medium	Moderate system knowledge training over months; refresher training required on a frequent basis (e.g. monthly or quarterly).
1	Low	Limited system knowledge training over days; refresher training required on a periodic basis (e.g. annually, biennially, or longer interval).
PSF		PURPOSE
HUMAN OPERATOR BEHAVIOR TYPE		Determine the type of human operator behavior (SRK) in executing the task.
RANK	ASSESSMENT	CRITERIA
3	Knowledge	Task requires significant knowledge-based behavior.
2	Rule	Task is executed in accordance with a flight rule or documented procedure.
1	Skill	Task is entirely skill-based (e.g. "stick and rudder")
PSF		PURPOSE

TASK PROCEDURES		Determine if the procedures associated with the task are defined to the correct level of operational detail.
RANK	ASSESSMENT	CRITERIA
3	Deficient/ Absent	Procedure is either non-existent or is very complicated (number of steps), has inappropriate detail (too much or too little), requires significant knowledge-based behavior, is confusing or verbose, or is inaccurate.
2	Moderate	Procedure is moderately complicated (number of steps), has some inappropriate detail, requires some knowledge-based behavior, is overly verbose, or contains some inaccuracies.
1	Comprehensive	Procedure is simple and uncomplicated, has appropriate detail, requires no knowledge-based behavior, has the correct level of verbosity, and is accurate.
PSF		PURPOSE
IMPACT OF UNENGAGED HUMAN OPERATORS		Determine the level of consequential impact with respect to how quickly a human operator could regain situational awareness during or after task execution, assuming a report of the executed timeline, current status, and recent state changes provided.
RANK	ASSESSMENT	CRITERIA
3	High	<ul style="list-style-type: none"> • Display information may not be sufficient for operator to regain situational awareness; • Downlink or data dumps of additional information are required to regain situational awareness; integration of information with flight crew, ATC, and company dispatch is required to regain situational awareness; • If a fault, failure, or off-nominal condition or event occurs during the task execution and deep systems knowledge and operator knowledge-based decision-making are required with a short time to effect to reach a safe state; • Flight crew response is required with a short time to effect to achieve the goal state. • Probability of a negative transfer of training from a similar system.
2	Medium	<ul style="list-style-type: none"> • Display information along with review of executed tasks is sufficient for operator to regain situational awareness; • Downlink or data dumps of additional information are required to regain situational awareness; • Integration of information between the flight crew and ATC is required to regain situational awareness; or • If a fault, failure, or off-nominal condition or event occurs during the task execution, systems knowledge and operator knowledge-based decision-making may be required to reach a safe state. • Possibility of a negative transfer of training from a similar system.
1	Low	<ul style="list-style-type: none"> • Report information is sufficient for operator to regain situational awareness; • Little to no integration of information with one other Liveware entity (ATC or Dispatch) is required to regain situational awareness; • If a fault, failure, or off-nominal condition or event occurs during the task execution, the system can remain in its safed state until further recovery actions are decided. • Unlikely that a negative transfer of training from a similar system will occur.
PSF		PURPOSE

HUMAN-MACHINE INTERFACE (HMI)		Determine which HMI will be used to perform the task.
RANK	ASSESSMENT	CRITERIA
3	Complex Autoflight	Task will be performed by the crew by programming of the FMS while in flight (e.g., RWY approach change).
2	Primary Autoflight	Task will be performed by the crew using primary autoflight controls (HDG, ALT, NAV, APPR, N1, A/S, A/T etc.).
1	Flight Controls	Task will be performed by the flight crew using manual inputs to the primary and secondary flight controls.

TABLE 7
HIERARCHY OF CONTROL EFFECTIVENESS

① ELIMINATION – discard the task.	
② SUBSTITUTION – substitute a complex task for a simpler one or change to a different interface for this task.	
③ ENGINEERING CONTROL – reengineer the system to be less error provocative or make the error easier to detect (increase error prevention and tolerance).	
④ FLIGHT RULE OR CONSTRAINT – establish a flight rule or constraint to prevent the error from occurring.	