How Do You Do Safety For Mili-Vilian Rotorcraft?

Presented to the
Tennessee Valley Chapter of the System Safety Society
On 15 July 2015
By
Steven R. Hosner
System Safety Engineering, LLC
Hosnersr_pe@knology.net 256-655-6323
Introduction

*Mili-Vilian rotorcraft are:
• Rotorcraft built under military contract
• Required to be acceptably safe for operations in:
  • Military controlled airspace, AND
  • FAA controlled airspace

*No, mili-vilian rotorcraft are not multi-legged, evil helicopters!
Introduction

• Accommodations for both the military (MIL-STD-882) and the civil (FAA) system safety approaches are necessary so the aircraft will be considered acceptably safe for flight in both civil and military airspaces.

• Safety information should be fed between the approaches to make sure they are synchronized (e.g. between the draft/preliminary Aircraft Safety Assessment Report and the Aircraft Functional Hazard Assessment).
Introduction

• This accommodation:
  • Harmonizes the hazard severity definitions from both domains
  • Applies the appropriate system safety requirements to functional hazards based on the domain the functions come from (military (e.g. weapons) versus civilian (RNP))
  • Uses a top-down functional approach until you reach implementations when you can switch over to MIL-STD-882 implementation-oriented approach
Hazard Severity Definitions

• One possible harmonization of the hazard severity definitions is shown on the next slide

• The differences are caused by the point of view of the two approaches:
  • Civil – Government regulator concerned with public safety
  • Military – Owner, Operator, Integrator, Developer, Maintainer
<table>
<thead>
<tr>
<th>Category</th>
<th>Term</th>
<th>Effect on aircraft</th>
<th>Effect on safety</th>
<th>Effect on personnel</th>
<th>Effect on crew and workload</th>
<th>Repair costs/ Maintenance Impacts</th>
<th>Mission Effects</th>
<th>Environmental concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military</td>
<td>I</td>
<td>Catastrophic</td>
<td>Loss of aircraft</td>
<td>Safety of Flight</td>
<td>Could result in one or more fatalities, permanent total disability</td>
<td>Physical distress or excessive workload impairs ability to perform tasks to the point where it prevents continued safe flight and landing</td>
<td>Damage and/or repair costs exceeding 50% of aircraft value or exceeding $2 M, whichever is greater</td>
<td>Irreversible severe environmental damage that violates law or regulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Civil (public safety) and Military (owner)</td>
<td>or unable to continue safe flight and landing</td>
<td>Civil (public safety) and Military (Operator)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>II</td>
<td>Critical</td>
<td>A large reduction in functional capability</td>
<td>A large reduction in safety margins (3 or more orders of magnitude increase in probability of failure, two level increase in severity)</td>
<td>Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel</td>
<td>Physical discomfort or large workload increase impairs crew ability to perform tasks accurately or completely or would cause the pilot to use emergency procedures</td>
<td>Damage and/or repair costs exceeding 10% but less than 50% of aircraft value or exceeding $400K but less than $2M, whichever is greater</td>
<td>Reversible environmental damage causing a violation of law or regulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Civil (public safety)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
System Safety Requirements

• In general, military probability of failure requirements are two orders of magnitude more probable than civilian requirements (e.g. military probability – $10^{-5}$ per hour, civil probability – $10^{-7}$ per hour)

• Level of Rigor is intended to be equivalent to Development Assurance Level (DAL)

• The next slide has an example of appropriate system safety requirements
### Example Program Target Acceptable Risk

<table>
<thead>
<tr>
<th>Hazard Severity</th>
<th>Negligible</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil</td>
<td>&lt;10^-3/hr</td>
<td>&lt;10^-5/hr</td>
<td>&lt;10^-7/hr</td>
<td>&lt;10^-9/hr</td>
</tr>
<tr>
<td>Military</td>
<td>&lt;10^-1/hr</td>
<td>&lt;10^-3/hr</td>
<td>&lt;10^-5/hr</td>
<td>&lt;10^-7/hr</td>
</tr>
<tr>
<td>DAL=D</td>
<td>LOR=4</td>
<td>DAL=C</td>
<td>LOR=3</td>
<td>DAL=A</td>
</tr>
<tr>
<td>LOR=1</td>
<td>DAL=A</td>
<td>LOR=2</td>
<td></td>
<td>LOR=1</td>
</tr>
</tbody>
</table>

**Example Program Target Acceptable Risk**

- **Negligible**
  - Civil: <10^-3/hr
  - Military: <10^-1/hr
- **Marginal**
  - Civil: <10^-5/hr
  - Military: <10^-3/hr
- **Critical**
  - Civil: <10^-7/hr
  - Military: <10^-5/hr
- **Catastrophic**
  - Civil: <10^-9/hr
  - Military: <10^-7/hr

**Hazard Severity**

- Negligible
- Marginal
- Critical
- Catastrophic
Aircraft Context

Aircraft – (UH-13 Hekawi) –
Aircraft Functional Model

- Navigation Aid
- Nav Aid Pos Info
- UH-13 Hekawi
- Info Dsplys(Nav (Hekawi Pos Dsply, Msldg Nav Info Wrng Dsply))

Crew
Aircraft – (UH-13 Hekawi) – Composed of one or more:
Aircraft-Level Functions – (Navigation)
Aircraft Level Of Design Functional Model

Nav Aid

Nav Aid Pos Info

Navigation

Electrical Power

Electrical

UH-13 Hekawi

Info Dsplys (Nav (Hekawi Pos Dsply, Msldg Nav Info Wrng Dsply))

Crew
Misleading Information

• AC 25-11A Definition

Misleading Information - Incorrect information that is not detected by the flight crew because it appears as correct and credible information under the given circumstances. When incorrect information is automatically detected by a monitor resulting in an indication to the flight crew, or when the information is obviously incorrect, it is no longer considered misleading. The consequence of misleading information will depend on the nature of the information, and the given circumstances.
Aircraft-Level Function Level Of Design

Aircraft – (UH-13 Hekawi) Composed of one or more:
   Aircraft-Level Functions – (Navigation) Composed of one or more:
      Segments – (Navigation, Crew Vehicle Interface)

Aircraft-level function design decomposes the aircraft-level functions into segments
Aircraft-Level Function Level Of Design

- Navigation Aid
  - Position Information
- Flight Control Segment
- Propulsion Segment
- Navigation Aid
- IFF Interrogation
- IFF-Return
- ATC – Crew Communication
- Crew-ATC Communication
- Crew-Tactical Communication
- Tactical Units
- Tactical-Crew Communication
- Crew Vehicle Interface Segment
- Surveillance (IFF) Segment
- Electrical Power Segment
- Electrical power to all other Segments
- UH-13 Hekawi
- Air Pressure, Magnetic Lines of Force
- Flight Forces
- Crew Flight Plan Inputs (CFPI)
- Propulsion Control Inputs (PCI)
- Audio From Crew
- Audio To Crew
- Information Displays
- Primary Flight Indications
- Operational Environment
- Air Pressure, Magnetic Lines of Force

7/15/2015 3:25 PM
Functional System Safety Engineering Copyright Steven Hosner & David Schultz
Aircraft-Level Function Level Of Design

Functional Model

Navigation Aid

- Nav Aid Pos Info

**Navigation Segment**

- Nav Info(Hekawi Pos Data, Nav Data Status)

Dropped aircraft-level function
**Electrical** for simplicity

**Crew Vehicle Interface Segment**

- Crew

- Info Dsplys (Nav (Hekawi Pos Dsply, Msldg Nav Info Wrng Dsply))

Aircraft-Level Function **Navigation**

UH-13 Hekawi
Segment Level Of Design

Aircraft – (UH-13 Hekawi) Composed of one or more:
  Aircraft-Level Functions – (Navigation) Composed of one or more:
    Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:
      Systems – (Navigation Sensor System, ...)

Segment design decomposes the segment functions into systems
Aircraft – (UH-13 Hekawi) Composed of one or more:
  Aircraft-Level Functions – (Navigation) Composed of one or more:
    Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:
      Systems – (Navigation Sensor System, ...) Composed of one or more:
        Subsystems – (GPS Receiver Subsystem, ...)

System design decomposes the system functions into subsystems
System Level Of Design Functional Model

Navigation Sensor System

GPS Rcvr Subsys

GPS Pos Data, GPS Status Data

Navigation Data Correlator

Nav Snsr Data (Nav Snsr Pos Data (Corr Pos Data), Nav Data Status (GPS Data Status))

Position Estimation System

Nav Info (Hekawi Pos Data)

Nav Aid Pos Info

Info Dsplys (Nav (Hekawi Pos Dsply, Msldg Nav Info Wrng Dsply))

Crew Vehicle Interface Segment

Crew

Navigation Aid

Aircraft-Level Function Navigation

UH-13 Hekawi

7/15/2015 3:25 PM

© System Safety Engineering, LLC
Subsystem Level Of Design

Aircraft – (UH-13 Hekawi) Composed of one or more:
  Aircraft-Level Functions – (Navigation) Composed of one or more:
    Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:
      Systems – (Navigation Sensor System, ...) Composed of one or more:
        Subsystems – (GPS Receiver Subsystem, ...) Composed of one or more:
          Implementations – (Acme AG-72 GPS Receiver System, ...)

Subsystem design decomposes the subsystem functions into implementations
Aircraft Design

Aircraft - (UH-13 Hekawi)
Aircraft Functional Model

Navigation Aid -> Nav Aid Pos Info

UH-13 Hekawi

Info Dsplys(Nav (Hekawi Pos Dsply, Msldg Nav Info Wrng Dsply))

Crew
A draft Aircraft Functional Hazard Assessment (AFHA) will contain the aircraft’s:

- Functional model defining the interfaces between the aircraft and functions external to the aircraft
- Hazard analyses covering all aircraft functional interface hazards

We will concentrate on the Hekawi functional interfaces relevant to the Hekawi function of providing Information Displays (Navigation)
Aircraft Functional Hazard Analysis

Haz Svrtty: Critical
Pf = 10^-7 /hr
LOR/DAL = 2/B

Haz Svrtty: Critical
Pf = 10^-7 /hr
LOR/DAL = 2/B

We will concentrate on this one
Aircaft – (UH-13 Hekawi) Composed of one or more:
   Aircraft-Level Functions – (Navigation, Electrical)
ARP4761 Documentation Tie-In

• An interim/final AFHA will contain the aircraft level of design’s:
  • Allocation of aircraft functions to one or more aircraft-level functions
  • Functional models defining the interfaces between:
    • The aircraft-level functions themselves
    • The aircraft-level functions and functions external to the aircraft
  • Hazard analyses covering all aircraft-level function functional interface hazards
Aircraft Level Of Design Functional Hazard Analysis

Haz Svrt: Critical
Pf = 10-7 /hr
LOR/DAL = 2/B

Nav Aid Prov Un Mslg Nav Aid Pos Info To Hekawi
HEKPUMIDNC0

AC Lvl FN Nav Pro Un Mslg Info Dsplys (Nav(Hek Pos Dsply, Mslg Nav Info Wrng Dsply)) To Crew
HEKPUMIDNC13

AC Lvl FN Electrical Pro Out Of Tol Electical Power to AC Lvl FN Nav
HEKPUMIDNC15

We will concentrate on this one
Aircraft Level Of Design Functional Hazard Analysis

AC Lvl FN Nav Pro Un MsIdg Info Dsply(Nav(Hek Pos Dsply, MsIdg Nav Info Wrng Dsply)) To Crew

HEKPUMIDNC13

AC Lvl FN Nav Pro MsIdg Hekawi Pos Dsply To Crew

HEKPUMIDNC110

AC Lvl FN Nav Fails To Pro MsIdg Nav Info Wrnng Dsply To Crew

HEKPUMIDNC111

Haz Svrt: Critical
Pf = 10-7 /hr
LOR/DAL = 2/B

Haz Svrt: Critical
Pf = 10-5 /hr
LOR/DAL = 3/C

Haz Svrt: Marginal
Pf = 10-7 /hr
LOR/DAL = 2/B

We will concentrate on this one
Aircraft Level-Function Level Of Design

Aircraft – (UH-13 Hekawi) Composed of one or more:

Aircraft-Level Functions – (Navigation) Composed of one or more:
Segments – (Navigation, Crew Vehicle Interface)
Aircraft-Level Function Level Of Design Functional Model

- Navigation Aid
  - Nav Aid Pos Info
  - Navigation Segment
    - Nav Info (Hekawi Pos Data, Nav Data Status)
  - Dropped aircraft-level function Electrical for simplicity
- Crew Vehicle Interface Segment
- Aircraft-Level Function Navigation
- UH-13 Hekawi

Info Displys (Nav (Hekawi Pos Disply, Msldg Nav Info Wrng Disply))
ARP4761 Documentation Tie-In

• A Preliminary Aircraft Safety Assessment (PASA) will contain the aircraft-level function level of design’s:
  • Allocation of aircraft-level functions to one or more segments
  • Functional model defining the interfaces between:
    • The segments themselves
    • The segments and functions external to the aircraft-level function
  • Hazard analyses covering all segment functional interface hazards
Aircraft-Level Function Level Of Design Functional Hazard Analysis

AC Lvl FN Nav Fails To Pro MsIdg Nav Info Wrnng Dsply To Crew

Nav Seg Incorrectly Pro Nav Data Status Set To Good And Nav Seg Status (CBIT: Pass) To CVI Seg

CVI Seg Fails To Pro MsIdg Pos Data Wrnng Dsply To Crew

Haz Svrt: Critical
Pf = 10-7/hr
LOR/DAL = 2/B

We will concentrate on this one

© System Safety Engineering, LLC 37
Segment Level Of Design

Aircraft – (UH-13 Hekawi) Composed of one or more:
  Aircraft-Level Functions – (Navigation) Composed of one or more:
    Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:
      Systems – (Navigation Sensor System, ...)

© System Safety Engineering, LLC
DO-236 RNP, Figure 1-1 Navigation System Block Diagram

Navigation Aid

Position Information

Info Displays (Nav (Hekawi Pos Dsly, Msldg Nav Info Wrng Dsly))

Crew Vehicle Interface Segment

Nav Info (Hekawi Pos Data, Nav Data Status)

Aircraft-Level Function Navigation

UH-13 Hekawi
A Segment Functional Hazard Assessment will contain the segment level of design’s:

- Allocation of segment functions to one or more systems
- Functional model defining the interfaces between:
  - The systems themselves
  - The systems and the segment’s external interfaces
- Hazard analyses covering all system functional interface hazards
Segment Level Of Design Functional Hazard Analysis

Haz Svrty: Critical
Pf = 10-7 /hr
LOR/DAL = 2/B

Nav Seg Incorrectly Pro Nav Data Status Set To Good And Nav Seg Status (CBIT: Pass) To CVI Seg

HEKPUMIDNC1111

Nav Snsr Sys Incorrectly Pro Nav Data Status Set To Good And Nav Snsr Sys Status (CBIT: Pass) To Pos Est Sys

HEKPUMIDNC11113 Ext

Pos Est Sys Incorrectly Pro Nav Data Status Set To Good And Nav Snsr Sys Status (CBIT: Pass) To CVI Seg

HEKPUMIDNC11114 Ext

We will concentrate on this one
Aircraft – (UH-13 Hekawi) Composed of one or more:
  Aircraft-Level Functions – (Navigation) Composed of one or more:
    Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:
      Systems – (Navigation Sensor System, ...) Composed of one or more:
        Subsystems – (GPS Receiver Subsystem, ...)

System Level Of Design
Aircraft-Level Function Navigation

UH-13 Hekawi

Navigation Sensor System

Navigation Segment

GPS Rcvr Subsys

GPS Pos Data, GPS Status Data

Navigation Data Correlator

Nav Snsr Data (Nav Snsr Pos Data (Corr Pos Data (GPS Pos Dta)), Nav Data Status (GPS Dta Status))

Position Estimation System

Nav Aid Pos Info

Info Dsplys (Nav (Hekawi Pos Dsply, Msldg Nav Info Wrng Dsply))

Crew

Vehicle Interface Segment

Nav Info (Hekawi Pos Data, Nav Data Status)
ARP4761 Documentation Tie-In

• A Segment Preliminary System Safety Assessment will contain the system level of design’s:
  • Allocation of system functions to one or more specific system sub-functions and/or subsystems
  • Functional models defining the interfaces between:
    • The specific system sub-functions and subsystems
    • The specific system sub-functions, subsystems and functions external to the system
  • Hazard analyses covering all specific system sub-function and subsystem functional hazards
System Level Of Design Functional Hazard Analysis

NavSnsr Sys Incorrectly Pro Nav Data Status Set To Good And Nav Snsr Sys Status (CBIT: Pass) To Pos Est Sys

GPS Rcvr Sub Pro Undet MsIdg GPS Pos Data And Incrctly Pro GPS Rcvr Subsys Status Data (CBIT: Passed) To Nav Data Corr

Nav Data Corr Incrctly Pro Nav Data Status (Good) and Nav Snsr Sys Satus (GPS Status Data (CBIT: Passed)) To Pos Est Sys

We will concentrate on this one

Haz Svrt: Critical
Pf = 10^-7 / hr
LOR/DAL = 2/B
Aircraft – (UH-13 Hekawi) Composed of one or more:
- Aircraft-Level Functions – (Navigation) Composed of one or more:
  - Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:
  - Systems – (Navigation Sensor System, …) Composed of one or more:
  - Subsystems – (GPS Receiver Subsystem, …) Composed of one or more:
  - Implementations – (Acme AG-72 GPS Receiver System, …)
Misleading Information

• **Navigation Data Correlator** to implement the following logic:
  
  • **IF**
    
    • The difference between **GPSRS1 Position Data** and **GPSRS2 Position Data** > 2* Acme AG-72 GPS System position tolerance AND both **GPSRS1 CBIT Results** and **GPSRS2 CBIT Results** are set to Good
    
    • Then set **GPS Data Status** To Misleading
Misleading Information

Tolerance = 5 Units

\[ |\text{GPSRS1 Sensed Position} - \text{GPSRS2 Sensed Position}| > 2 \times \text{Tolerance} \]

The best that we can actually do is provide the crew with absolute certainty that they are lost because we have no way of knowing which case we are dealing with!
ARP4761 Documentation Tie-In

• A Subsystem Functional Hazard Assessment will contain the subsystem level of design’s:
  • Allocation of subsystems to one or more specific subsystem functions and/or implementations
  • Functional model defining the interfaces between:
    • Specific subsystem functions and implementations
    • Specific subsystem functions and implementations and functions external to the subsystem
  • Hazard analyses covering all specific subsystem function/implementation functional interface hazards
We will concentrate on this one
Subsystem Level Of Design
Functional Model

GPSRS Pro Undetectable Msldg GPSRS
GPS Pos Data and Incor Pro GPSRS
STatus Data(CBIT: Passed) To GPS Data Coll

HEKPUMIDNC111111203

GPSRS1 Pro Undet Msldg GPSRS1
Pos Data and Incor Pro GPSRS1
(CBIT:Passed) To GPS Data Coll

HEKPUMIDNC11111120330

GPSRS2 Pro Undet Msldg GPSRS2
Pos Data and Incor Pro GPSRS2
(CBIT:Passed) To GPS Data Coll

HEKPUMIDNC11111120331

Haz Svrt: Critical
Pf = 10-7/hr
LOR/DAL = 2/B

© System Safety Engineering, LLC
Subsystem Level Of Design Functional Model

Allocated:
Haz Svrt: Critical
Pf = 10-7 /hr
LOR/DAL = 2/B

GPSRS1 Pro Undet Msldg GPSRS1 Pos Data and Incor Pro GPSRS1 (CBIT:Passed) To GPS Data Coll
HEKPUMIDNC11111120330

Achieved Pf if allocated Pf achieved = 1X10-9 per hour

Haz Svrt: Critical
Pf = 10-5 /hr
LOR/DAL = 2/B

GPSRS1 Pro Undetectable Msldg GPSRS1 GPS Pos Data To GPS Data Collector
HEKPUMIDNC111111203300

Haz Svrt: Critical
Pf = 10-4 /hr
LOR/DAL = 2/B

Haz Svrt: Critical
Pf = 10-4 /hr
LOR/DAL = 2/B

Haz Svrt: Critical
Pf = 1 /hr
LOR/DAL = 2/B

|GPSRS1 GPS Pos Data Error| > GPSRS1 Accuracy
HEKPUMIDNC1111112033000 Ext

|GPSRS1 GPS Pos Data  -GPSRS2 GPS Pos Data| < 2 * GPSRS Accuracy
HEKPUMIDNC1111112033001 Ext

© System Safety Engineering, LLC 7/15/2015 3:25 PM 53
Top-Down Functional Approach

• At this point, the GPSRS1/2 hazard of concern (the provision of undetectable misleading GPS position data) and its safety requirements ($P_f = 1.0 \times 10^{-5}$ per hour, LOR/DAL = 2/B) can be passed to Acme Corporation as a top-level hazard and system safety requirement.

• The top-down approach can be followed further by Acme or the safety analysis/assessment approach can be switched to one of the MIL-STD-882 analyses.
Review

• The differences between the military (MIL-STD-882) and the civil (FAA) system safety approach are accommodated by:
  • Hazard severity definitions are harmonized
  • Safety requirements are defined based on the domain of the hazard (civil versus military domains)
Review

• The differences between the military (MIL-STD-882) and the civil (FAA) system safety approach are accommodated by:
  • Functional top-down methods are used to determine functional hazards
  • Functional hazard severities are assessed based on the harmonized definitions
  • Safety requirements are allocated to the functional hazard based on the domain of the hazard (civil versus military domains)
Review

• The differences between the military (MIL-STD-882) and the civil (FAA) system safety approach are accommodated by:
  • Safety requirements are allocated to implementations
  • Safety analysis/assessment of implementations use MIL-STD-882 analyses/assessments to determine residual risk
Questions, Discussion?
Backup Slides
Subsystem Level Of Design
Functional Model

• Navigation Data Correlator to implement the following logic:
  • IF
    • The difference between GPSRS1 Position Data and GPSRS2 Position Data > 2* Acme AG-72 GPS System position tolerance AND both GPSRS1 CBIT Results and GPSRS2 CBIT Results are set to Good
    • Then set GPS Data Status To Misleading
Subsystem Level Of Design
Functional Model

• **Navigation Data Correlator** to implement the following logic:
  • **Elseif**
    • The difference between **GPSRS1 Position Data** and **GPSRS2 Position Data** \(> 2 \times \) Acme AG-72 GPS System position tolerance AND either **GPSRS1 CBIT Results** or **GPSRS2 CBIT Results** are set to Failed
  • Then set **GPS Data Status To Good**
Subsytem Level Of Design Functional Model

• **Navigation Data Correlator** to implement the following logic:
  
  • **Elseif**
    
    • The difference between $\text{GPSRS}_1$ Position Data and $\text{GPSRS}_2$ Position Data $< 2 \times \text{Acme AG-72 GPS System position tolerance}$ AND one or neither $\text{GPSRS}_1$ CBIT Results and $\text{GPSRS}_2$ CBIT Results are set to Failed
  
  • Then set **GPS Data Status** To Good

  • **Else**
    
    • Set **GPS Data Status** To Bad