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

Category	Term Military	Effect on aircraft	Effect on safety Civil (public safety)	Effect on personnel (Civil and Military)	Effect on crew and workload Civil (public safety)	Repair costs/ Maintenance Impacts Military (owner, maintainer)	Mission Effects Military (Operator)	Environmental concerns Military (owner)
I	Catastrophic	Loss of aircraft Civil (public safety) and Military (owner)	Safety of Flight or unable to continue safe flight and landing	Could result in one or more fatalities, permanent total disability Civil (public safety) and Military (Operator)	Physical distress or excessive workload impairs ability to perform tasks to the point where it prevents continued safe flight and landing	Damage and/or repair costs exceeding 50% of aircraft value or exceeding $2 M, whichever is greater		Irreversible severe environmental damage that violates law or regulation
II	Critical	A large reduction in functional capability Civil(public safety)	A large reduction in safety margins (3 or more orders of magnitude increase in probability of failure, two level increase in severity)	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel	Physical discomfort or large workload increase impairs crew ability to perform tasks accurately or completely or would cause the pilot to use emergency procedures	Damage and/or repair costs exceeding 10% but less than 50% of aircraft value or exceeding $400K but less than $2M, whichever is greater	Immediate or almost immediate mission abort or emergency landing	Reversible environmental damage causing a violation of law or regulation

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

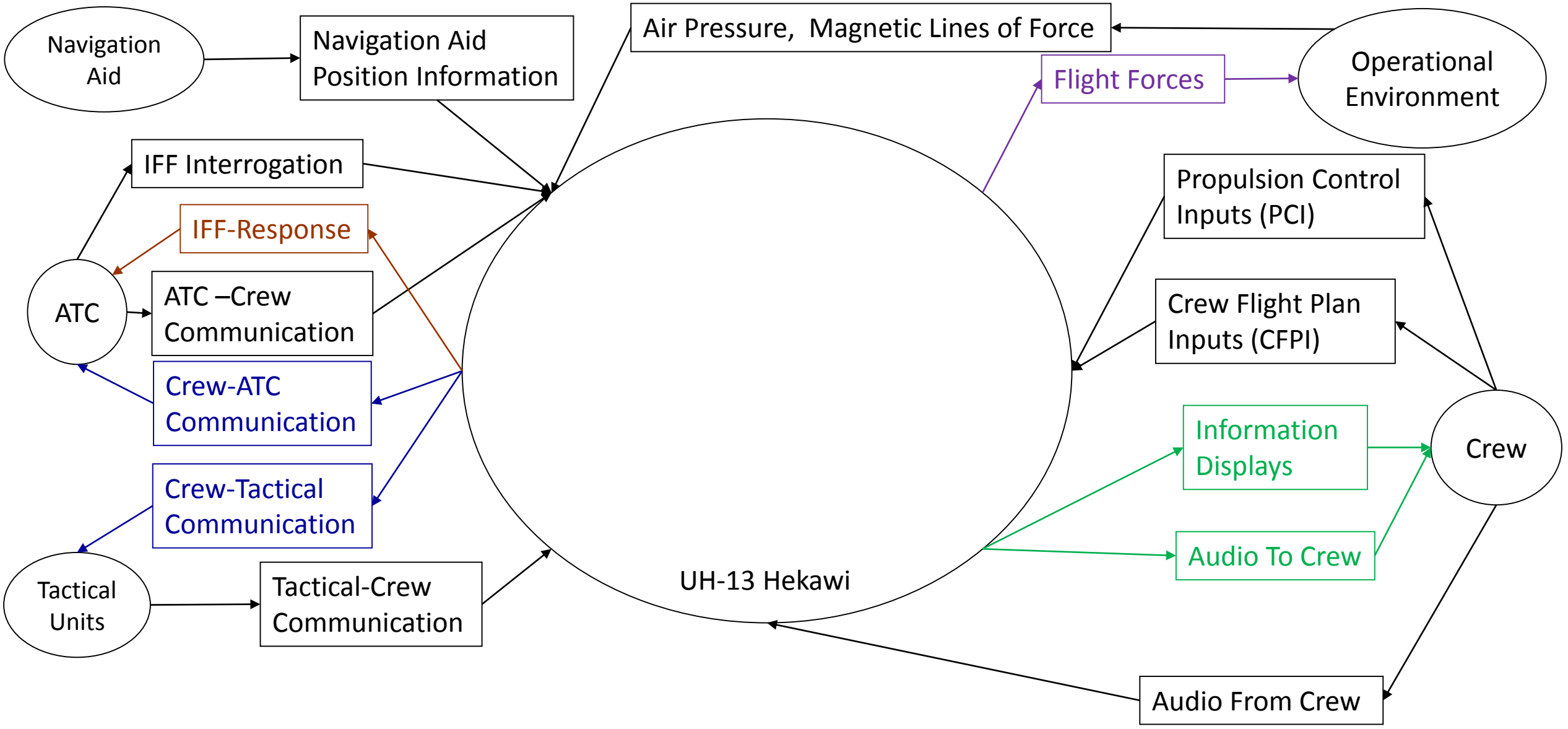
System Safety Requirements

Example Program Target Acceptable Risk							
Hazard Severity							
Negligible		**Marginal**		**Critical**		**Catastrophic**	
Civil	**Military**	**Civil**	**Military**	**Civil**	**Military**	**Civil**	**Military**
<10-3/hr DAL=D	<10-1/hr LOR=4	<10-5/hr DAL=C	<10-3/hr LOR=3	<10-7/hr DAL=B	<10-5/hr LOR=2	<10-9/hr DAL=A	<10-7/hr LOR=1

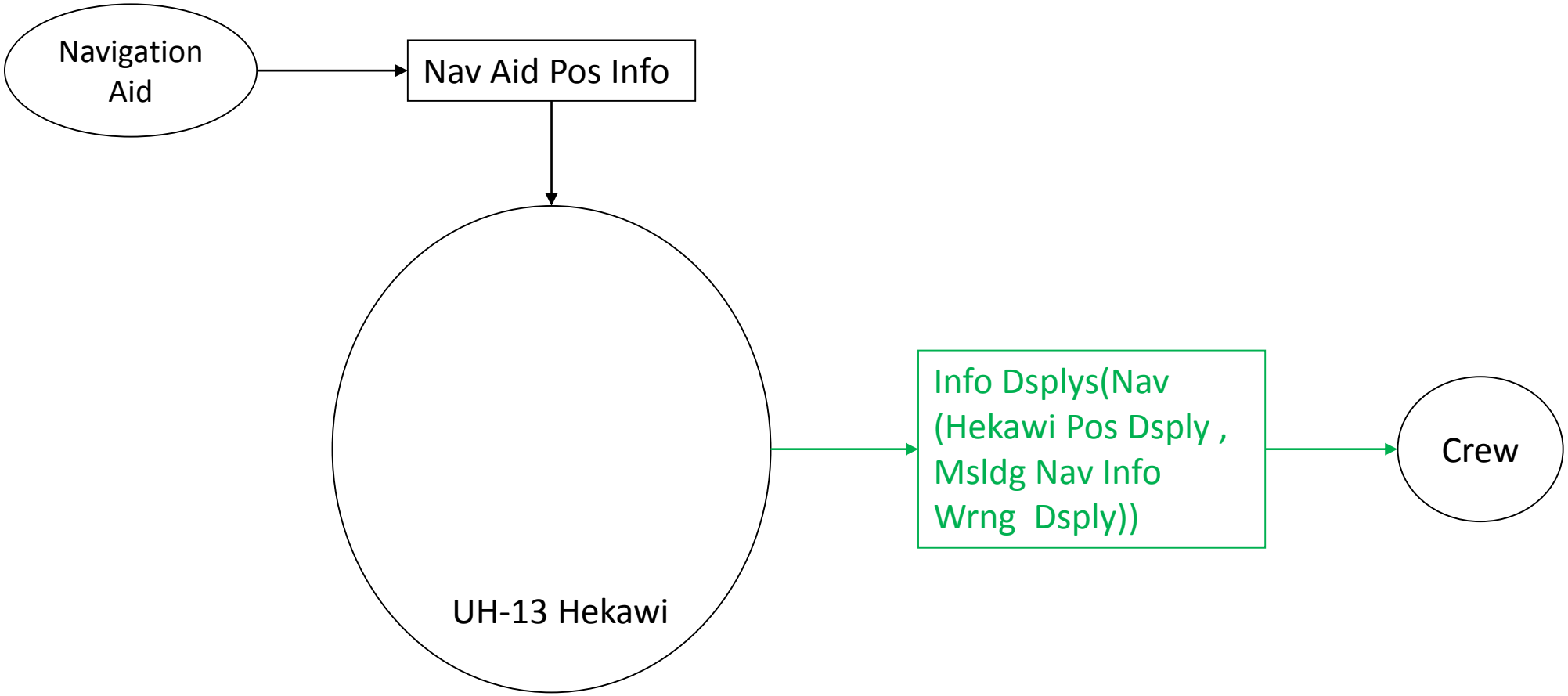
Aircraft Context

Aircraft – (UH-13 Hekawi) –

Aircraft Functional Model



Aircraft Functional Model

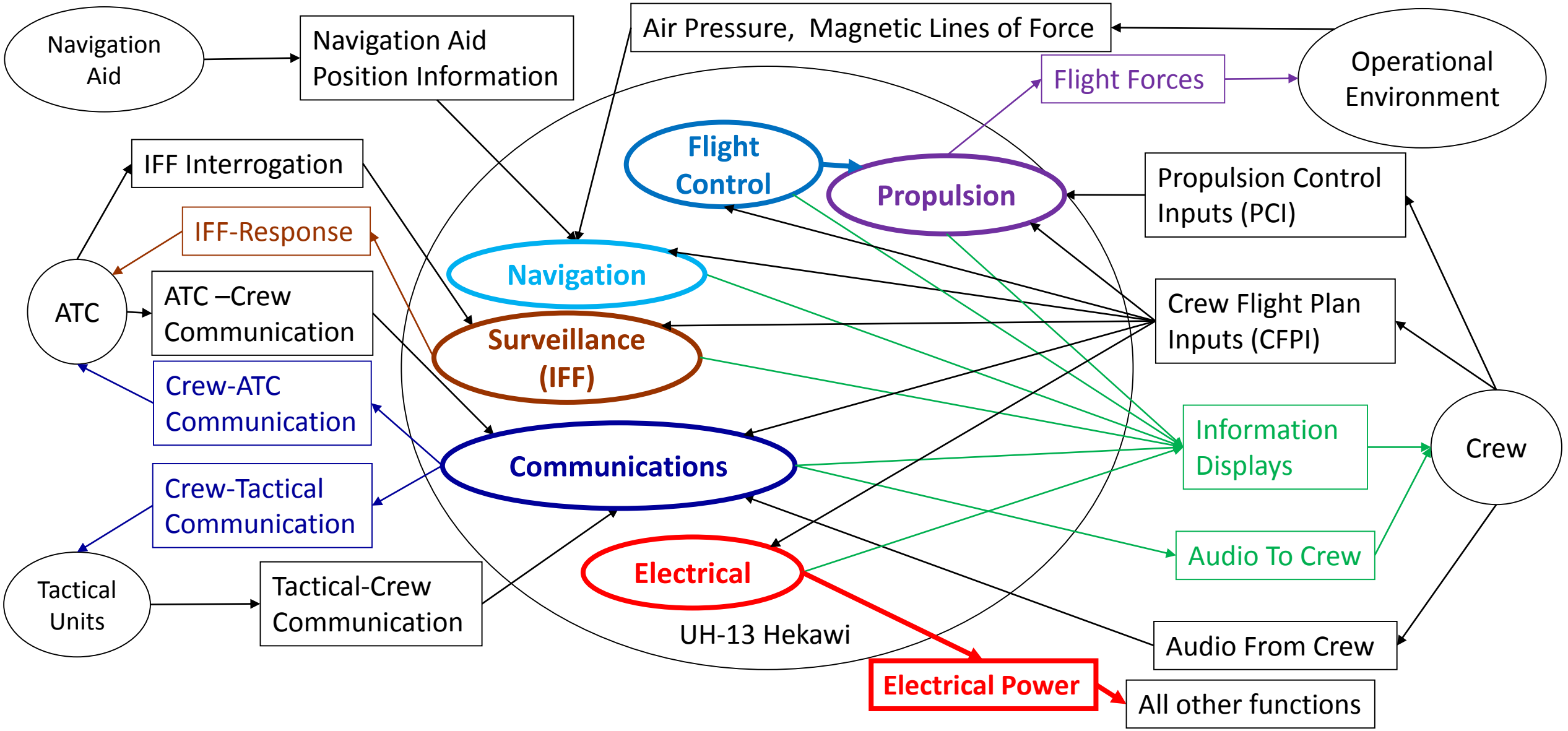


Aircraft Level Of Design

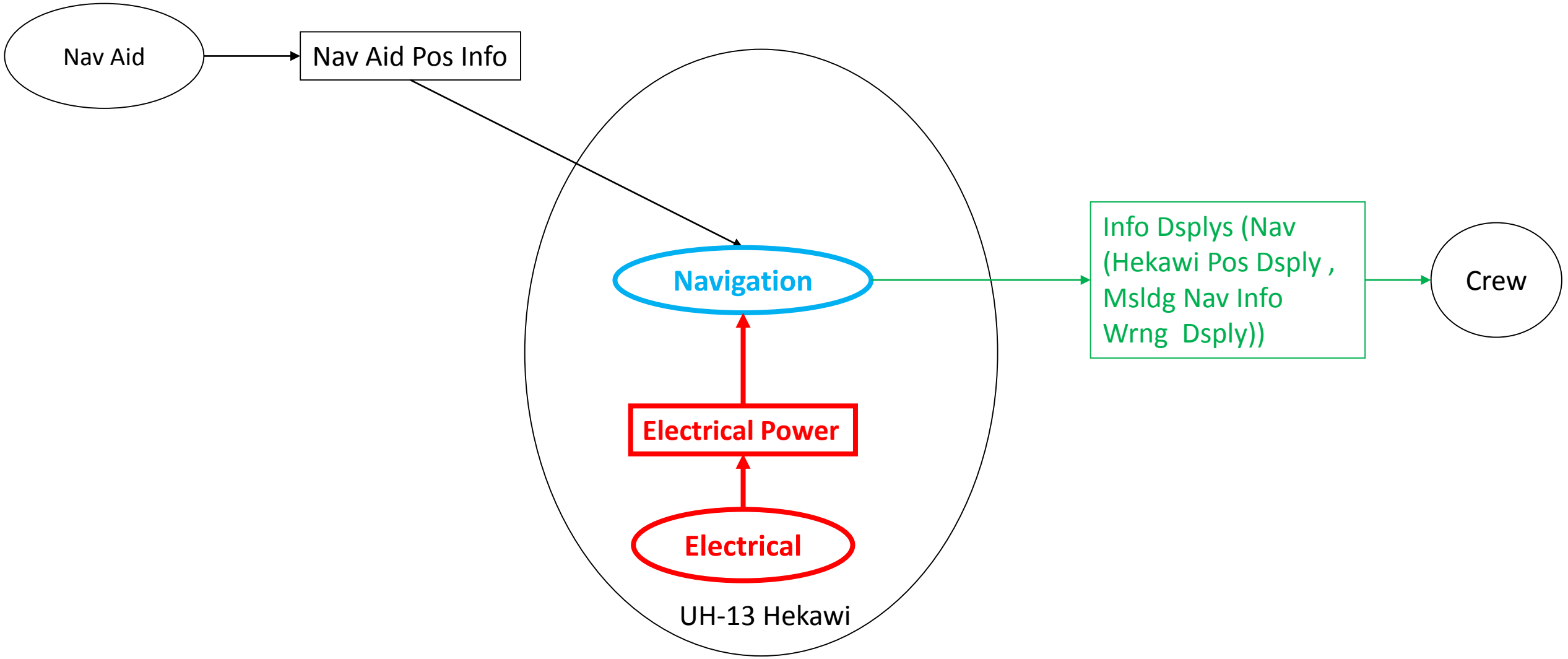
Aircraft – (UH-13 Hekawi) –Composed of one or more:

Aircraft-Level Functions – (Navigation)

Aircraft Level Of Design



Aircraft Level Of Design Functional Model



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

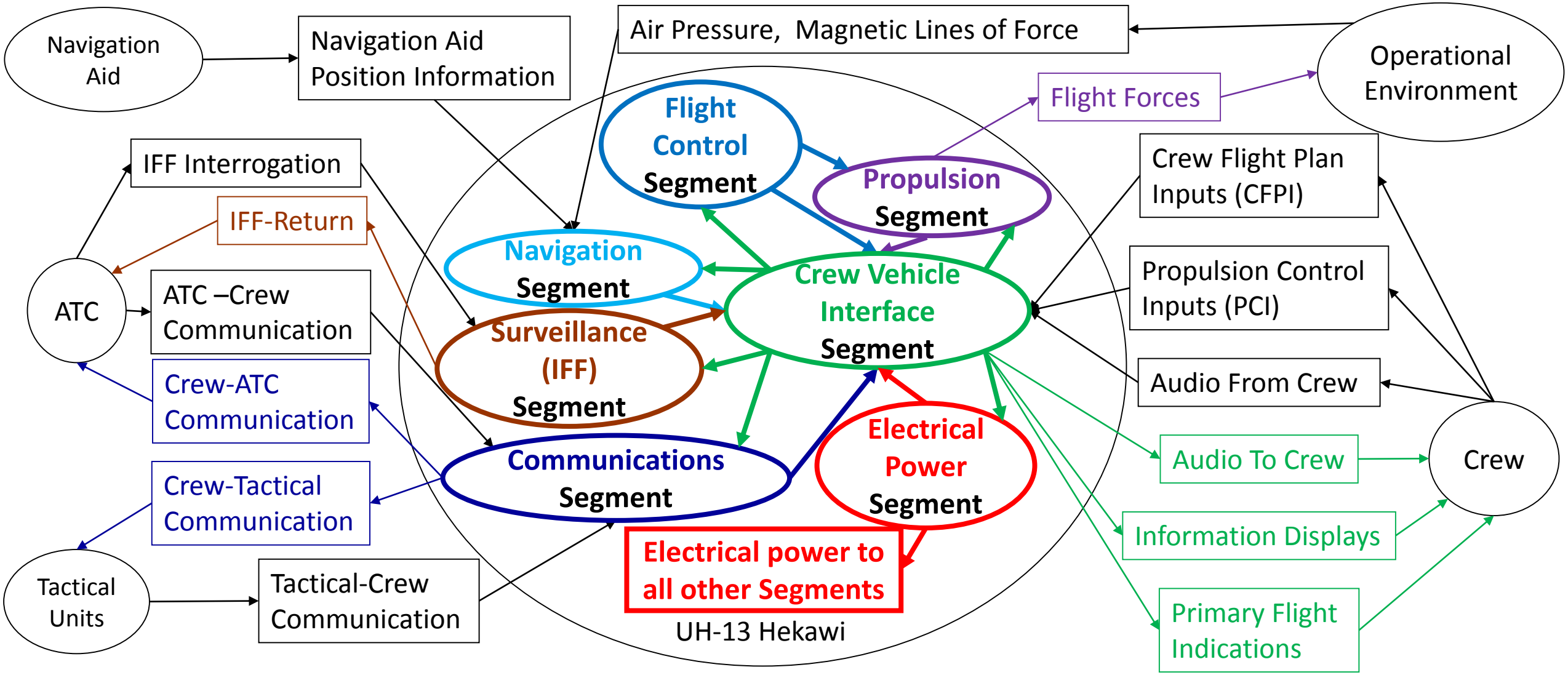
Aircraft – (UH-13 Hekawi) Composed of one or more:

Aircraft-Level Functions – (Navigation) Composed of one or more:

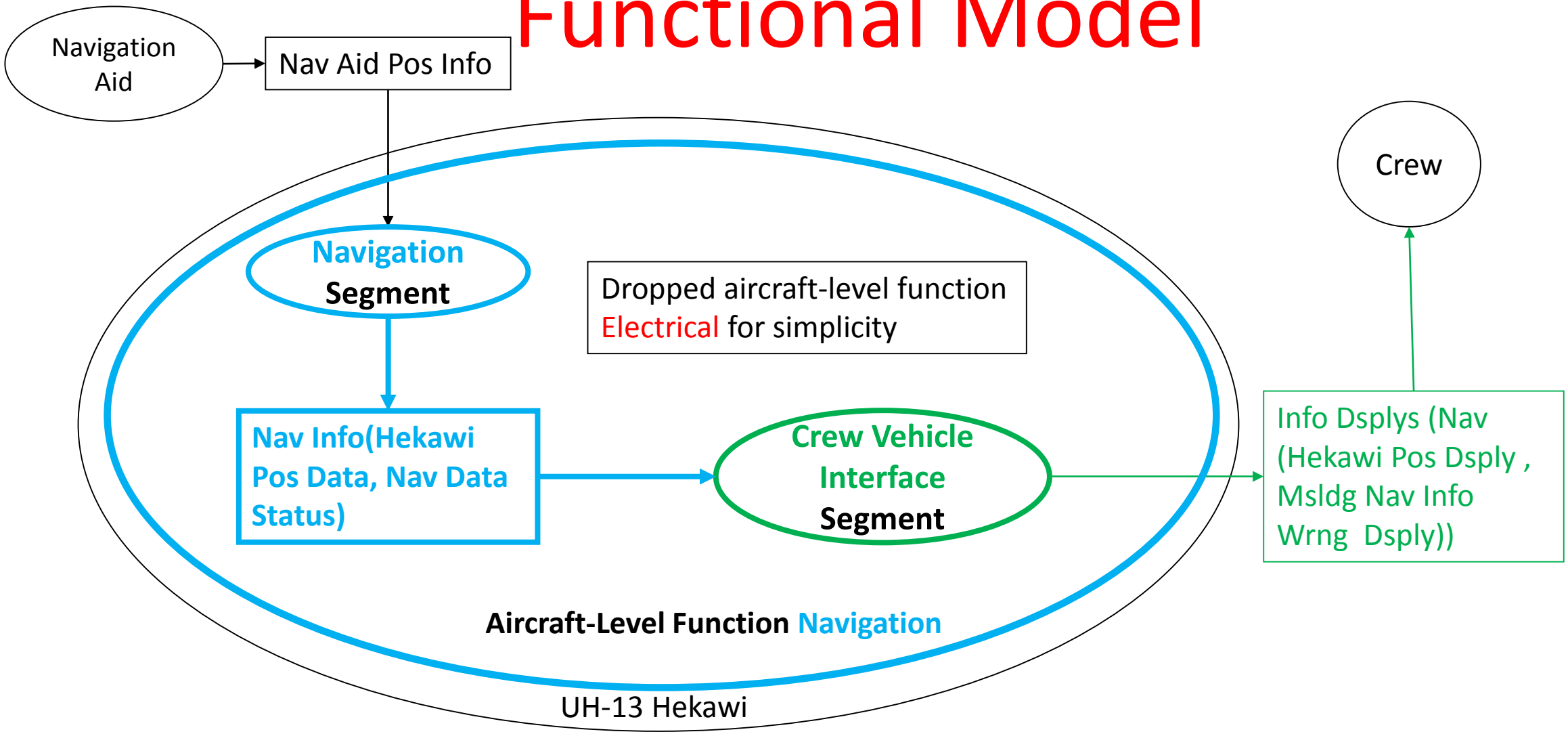
Segments – (Navigation, Crew Vehicle Interface)

Aircraft-level function design decomposes the aircraft-level functions into segments

Aircraft-Level Function Level Of Design



Aircraft-Level Function Level Of Design Functional Model



Segment Level Of Design

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

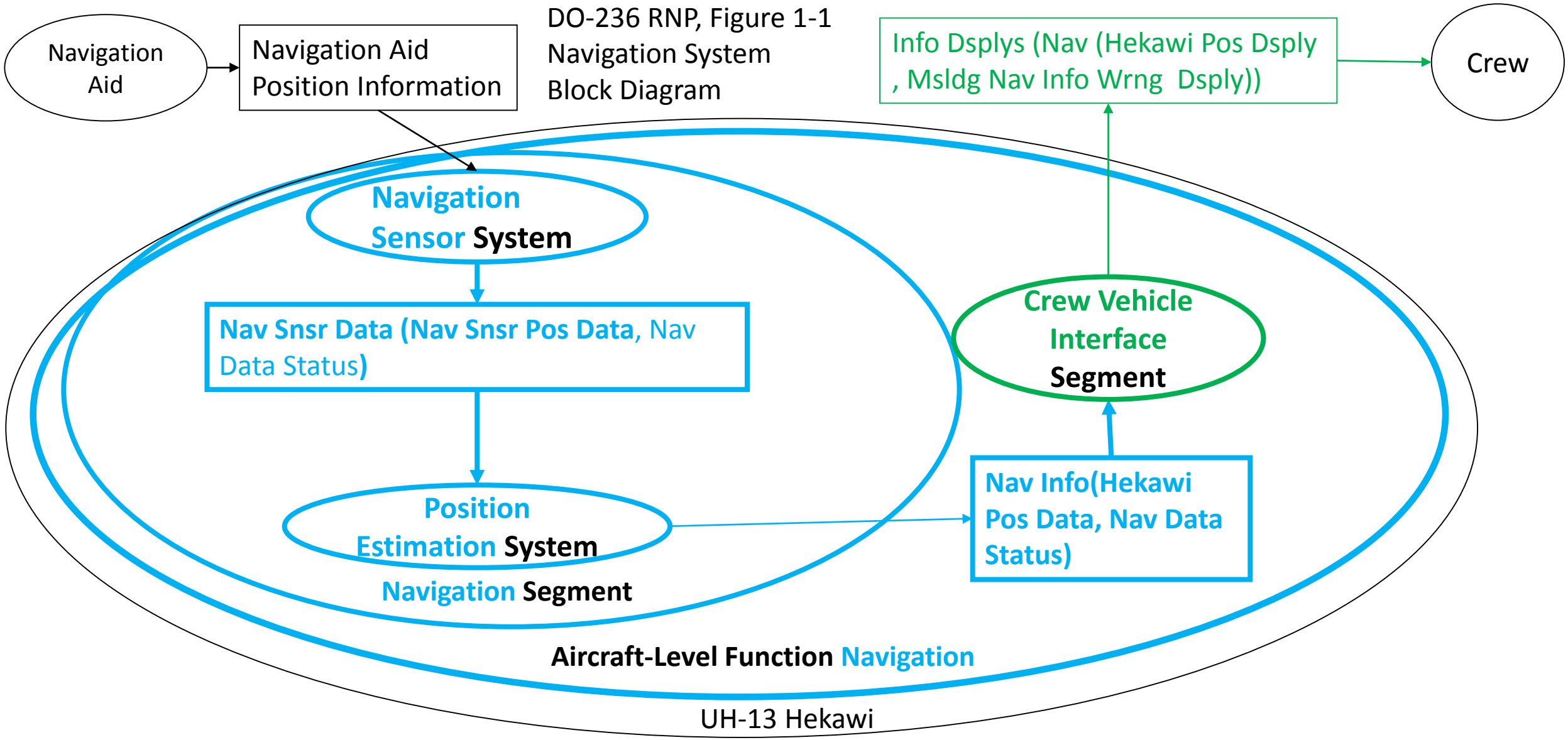
Aircraft-Level Functions – (Navigation) Composed of one or more:

Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:

Systems – (Navigation Sensor System, …)

Segment design decomposes the segment functions into systems

Segment Level Of Design Functional Model



System Level Of Design

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

Aircraft-Level Functions – (Navigation) Composed of one or more:

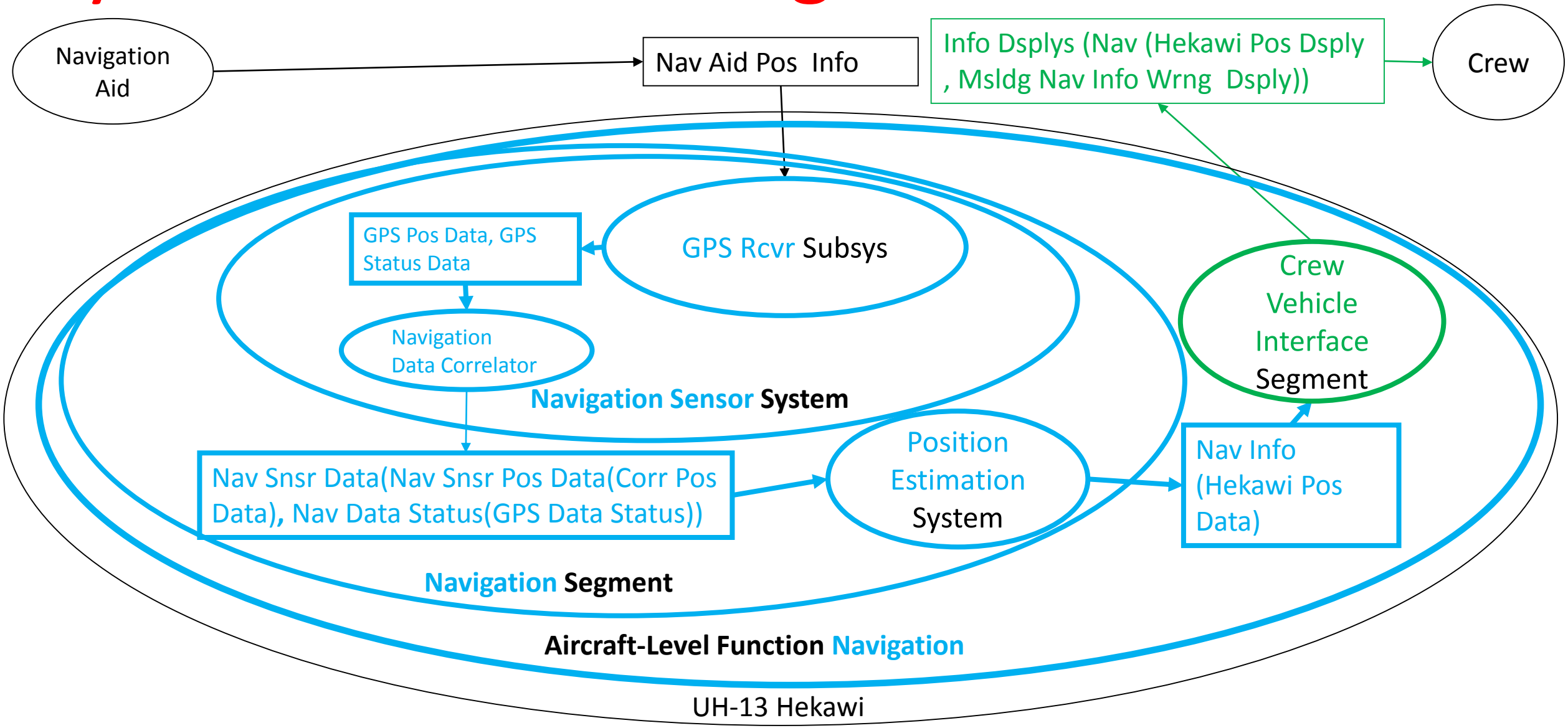
Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:

Systems – (Navigation Sensor System, …) Composed of one or more:

Subsystems – (GPS Receiver Subsystem, …)

System design decomposes the system functions into subsystems

System Level Of Design Functional Model



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:

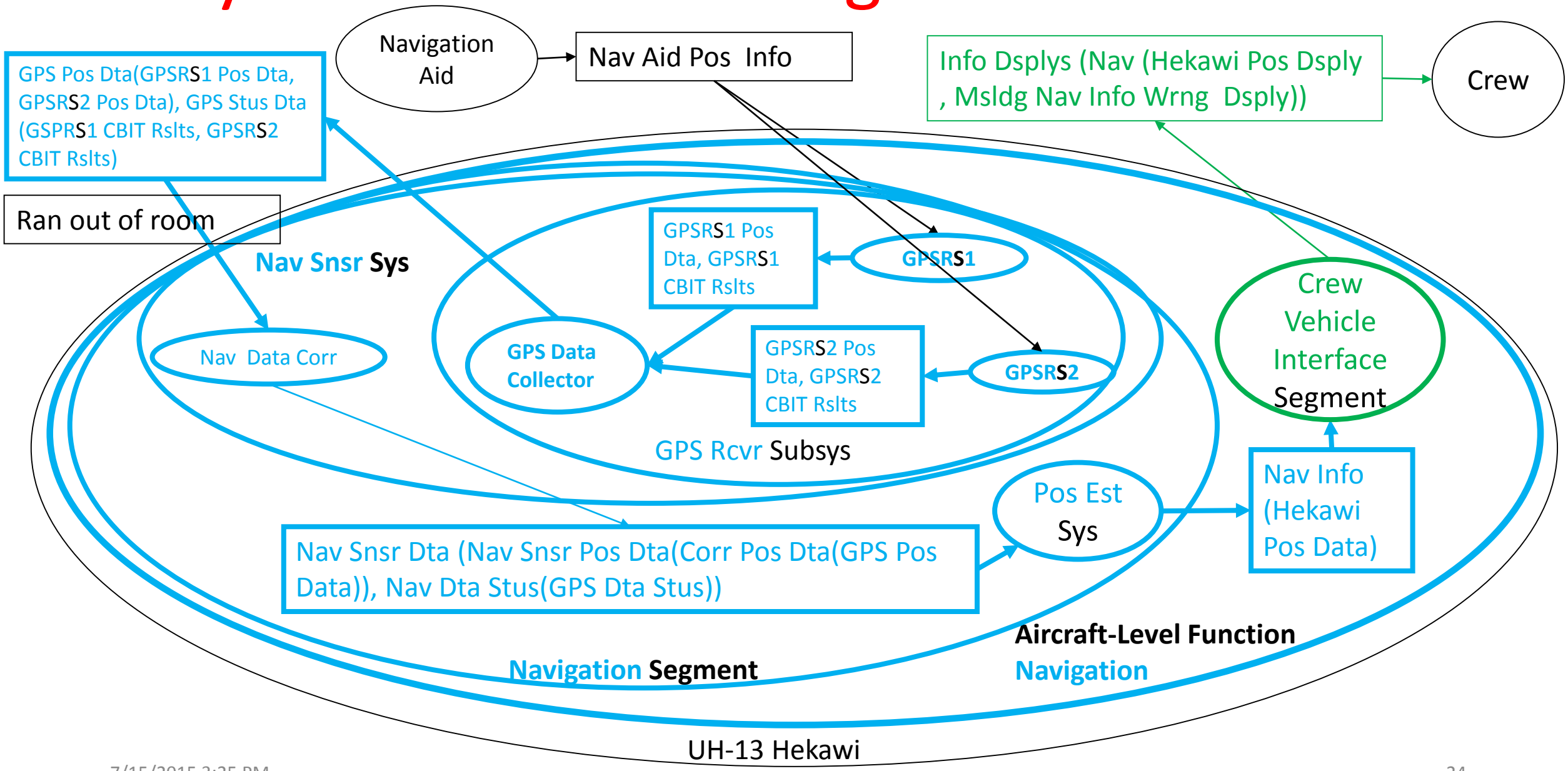
Systems – (Navigation Sensor System, …) Composed of one or more:

Subsystems – (GPS Receiver Subsystem, …) Composed of one or more:

Implementations – (Acme AG-72 GPS Receiver System, …)

Subsystem design decomposes the subsystem functions into implementations

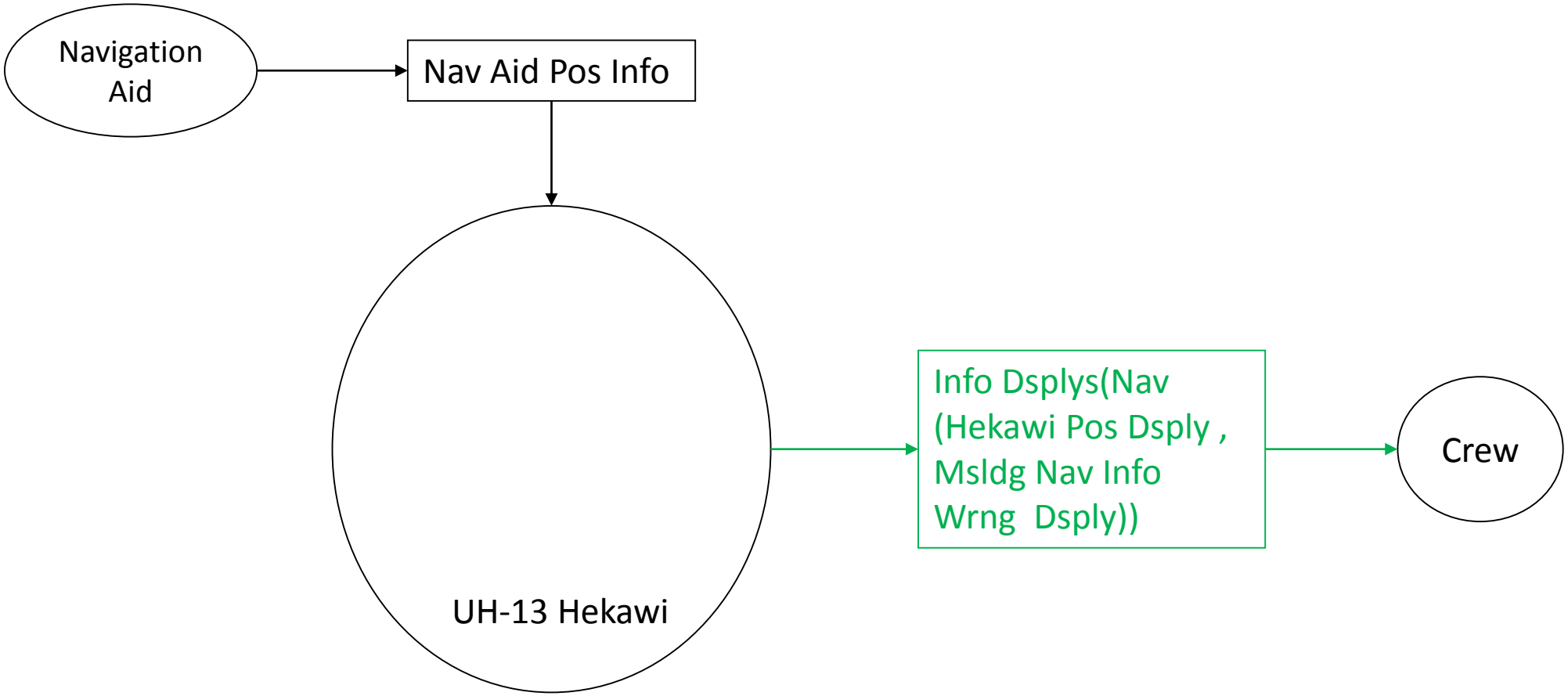
Subsystem Level Of Design Functional Model



Aircraft Design

Aircraft - (UH-13 Hekawi)

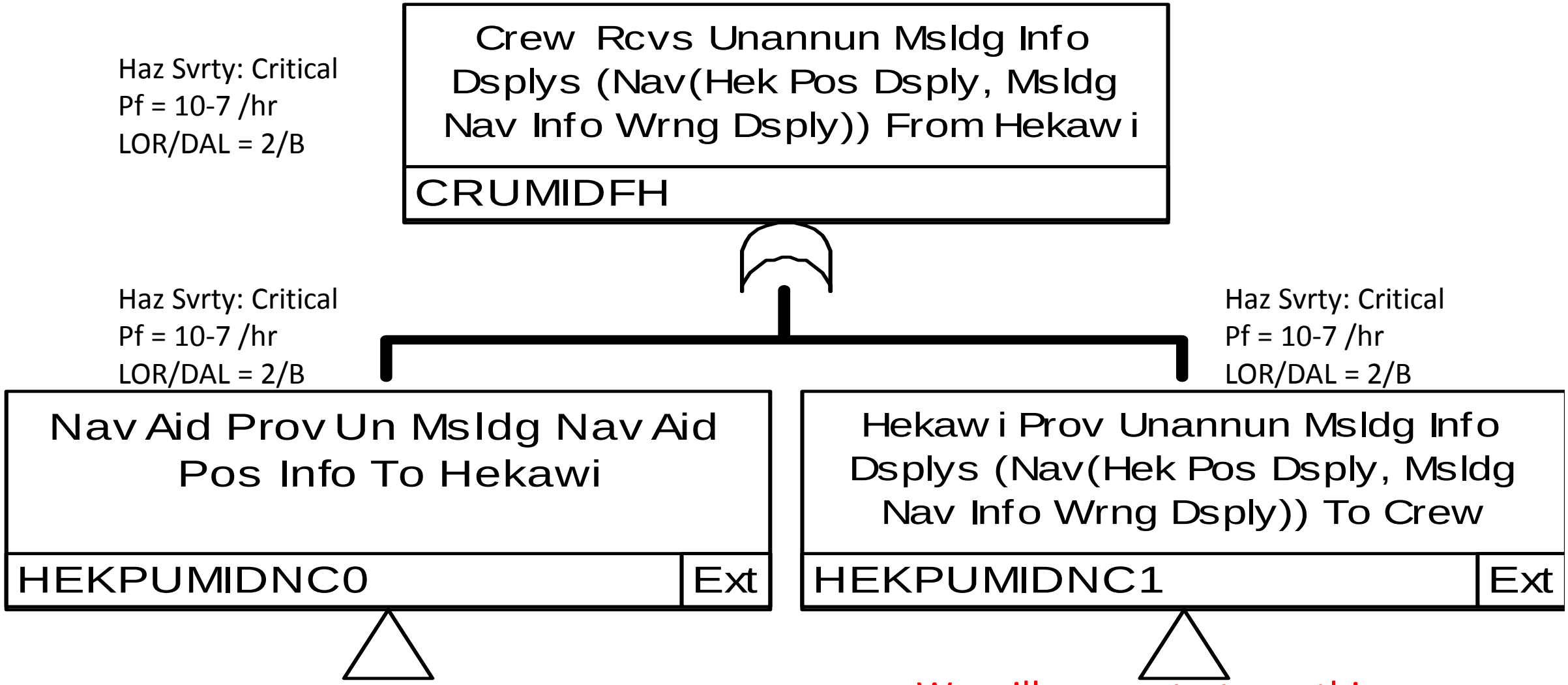
Aircraft Functional Model



ARP4761 Documentation Tie-In

- 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

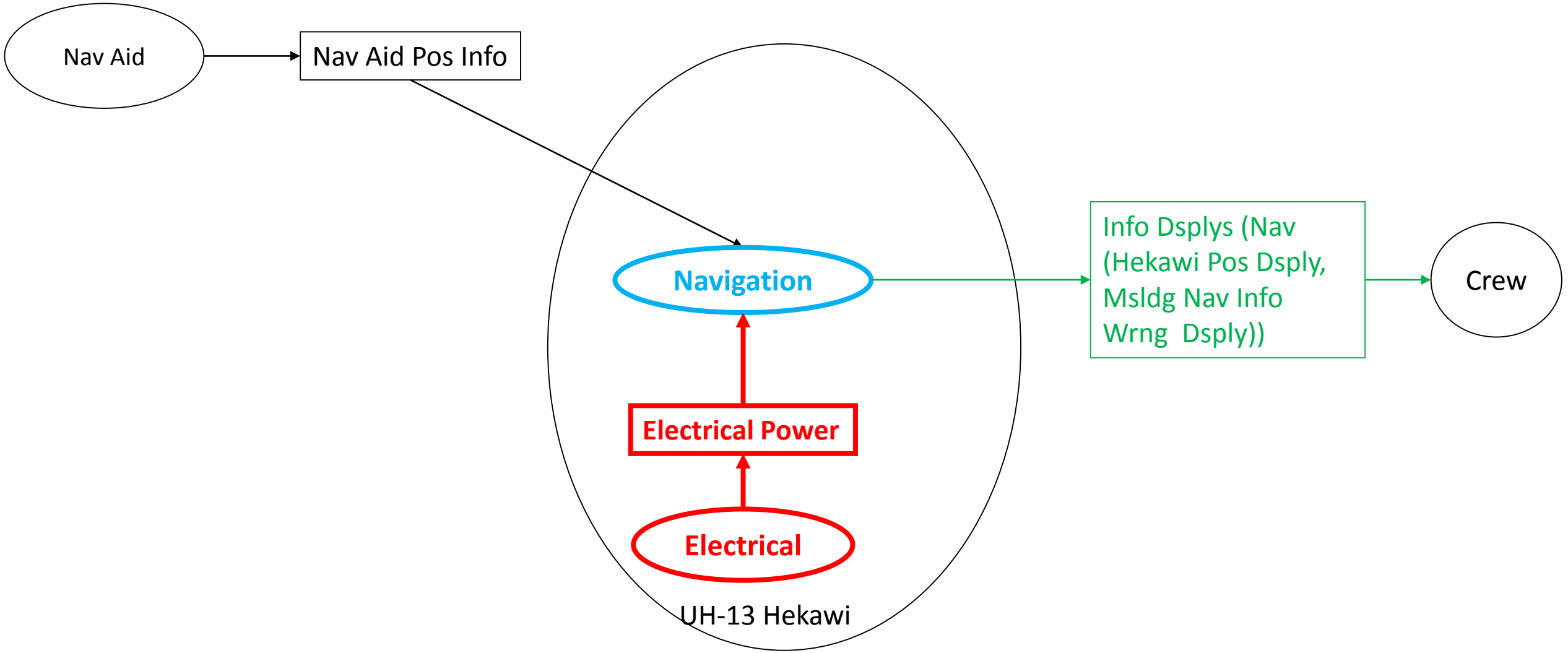


Aircraft Level Of Design

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

Aircraft-Level Functions – (Navigation, Electrical)

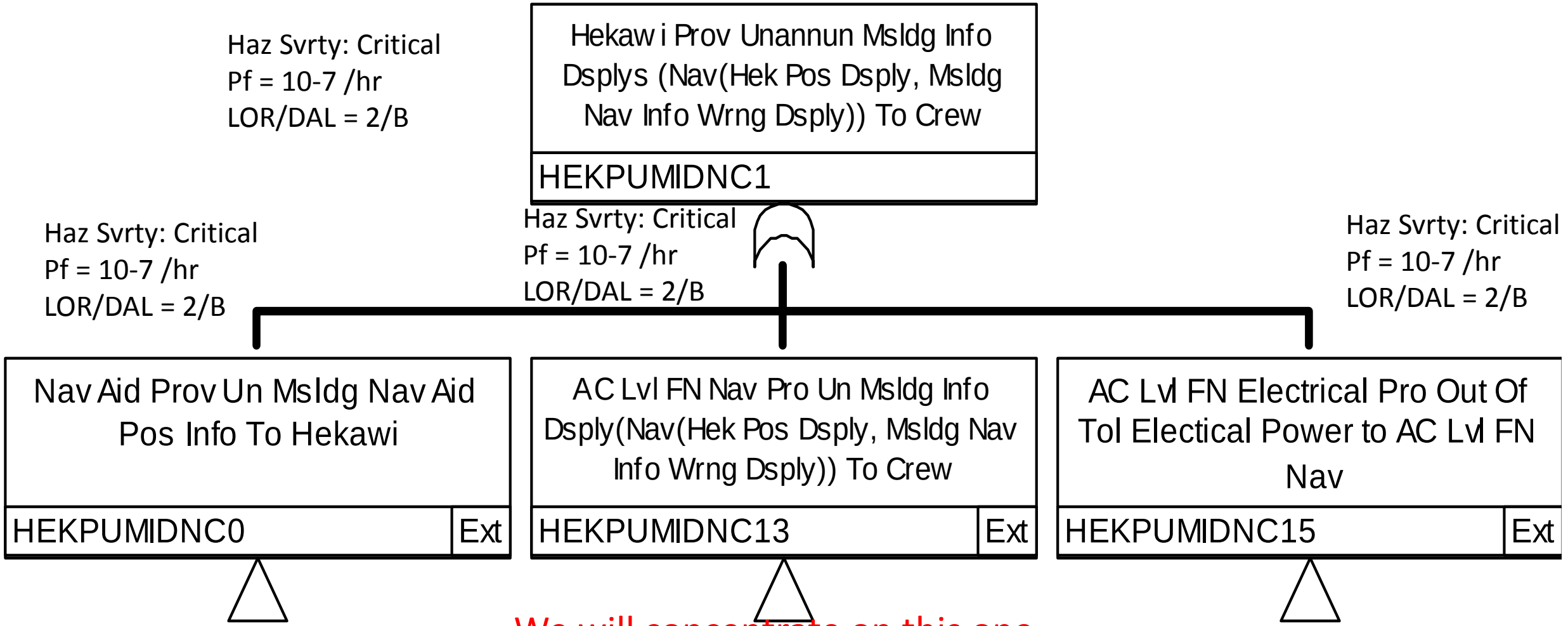
Aircraft Level Of Design Functional Model



ARP4761 Documentation Tie-In

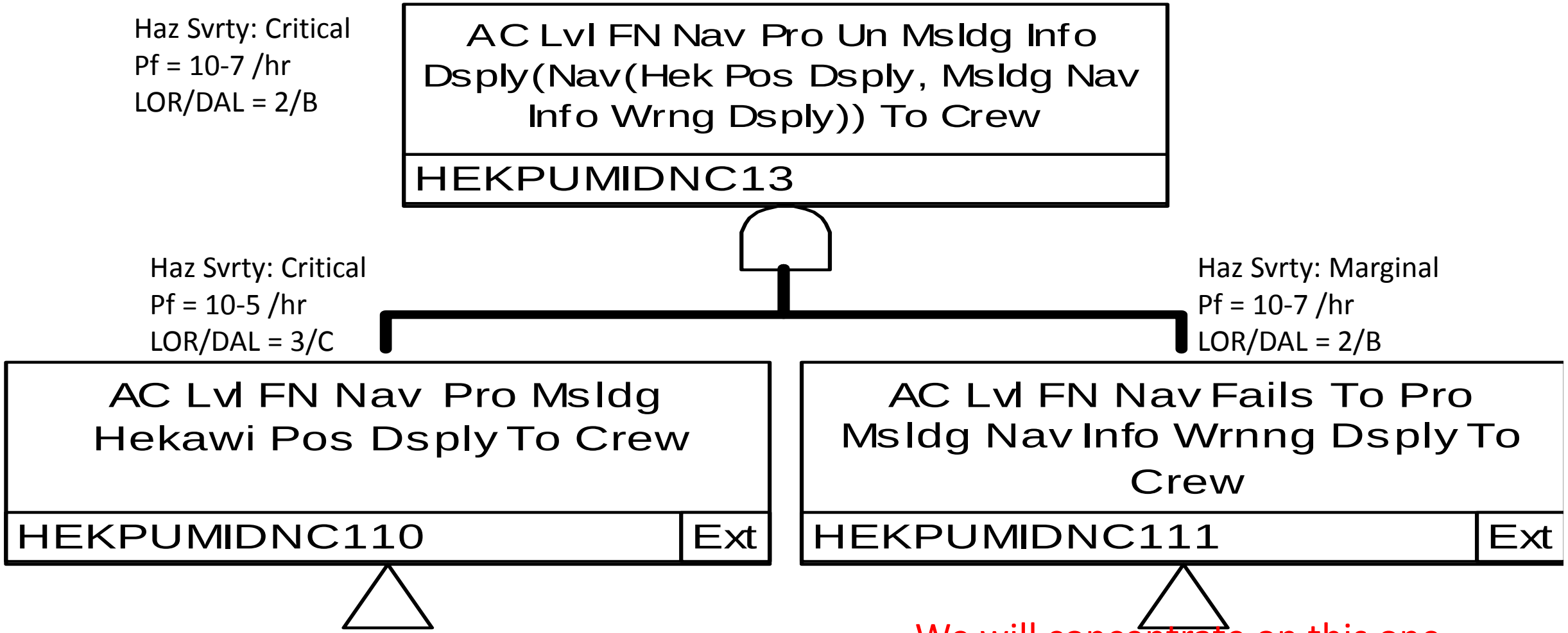
- An interim/final AFHA will contain the aircraft level of design's:
  - Allocation of aircraft functions to one or more aircraft-level functions
  - Functional models defining the interfaces between:
    - The aircraft-level functions themselves
    - The aircraft-level functions and functions external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

Aircraft Level Of Design Functional Hazard Analysis



We will concentrate on this one

Aircraft Level Of Design Functional Hazard Analysis



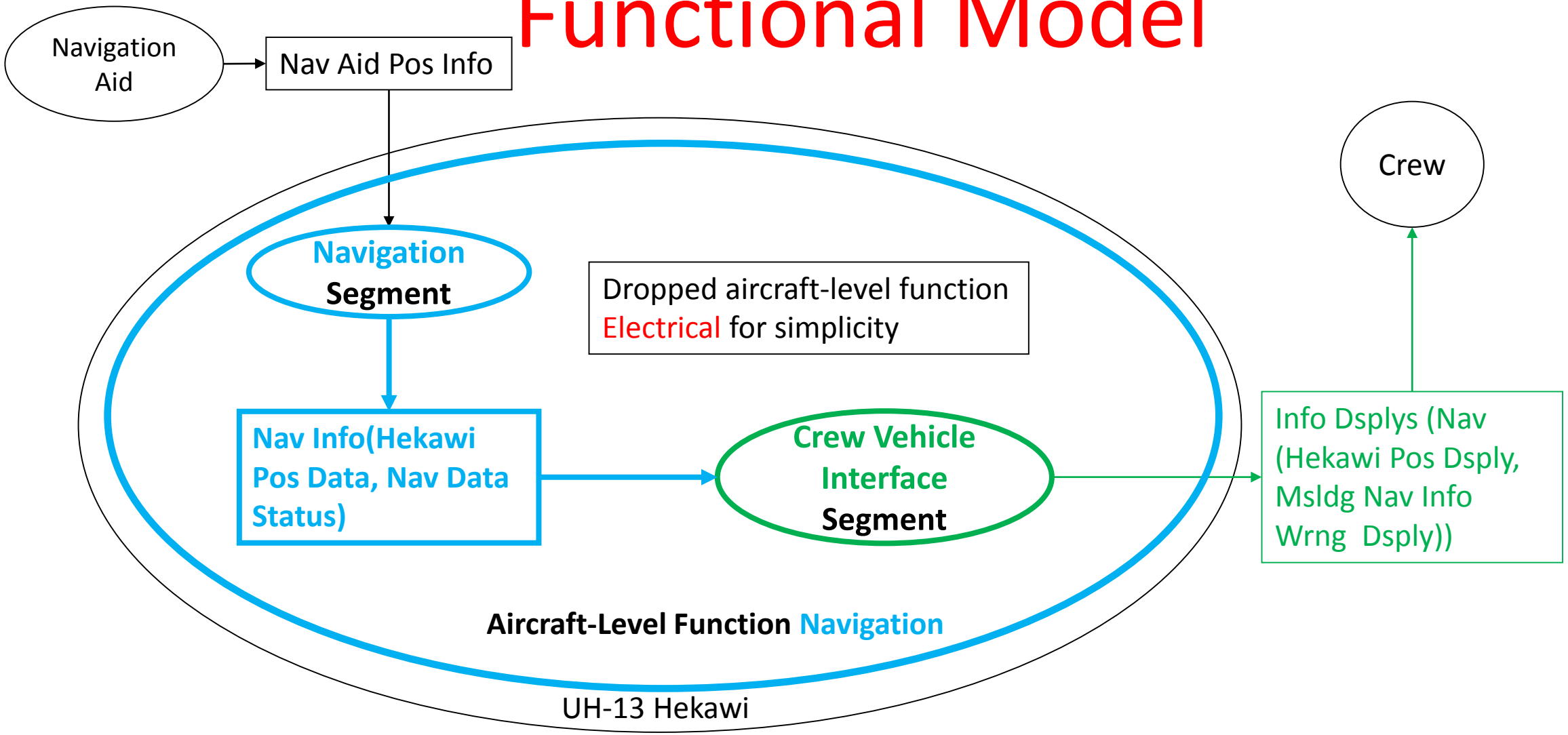
Aircraft Level-Function Level Of Design

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

Aircraft-Level Functions – (Navigation) Composed of one or more:

Segments – (Navigation, Crew Vehicle Interface)

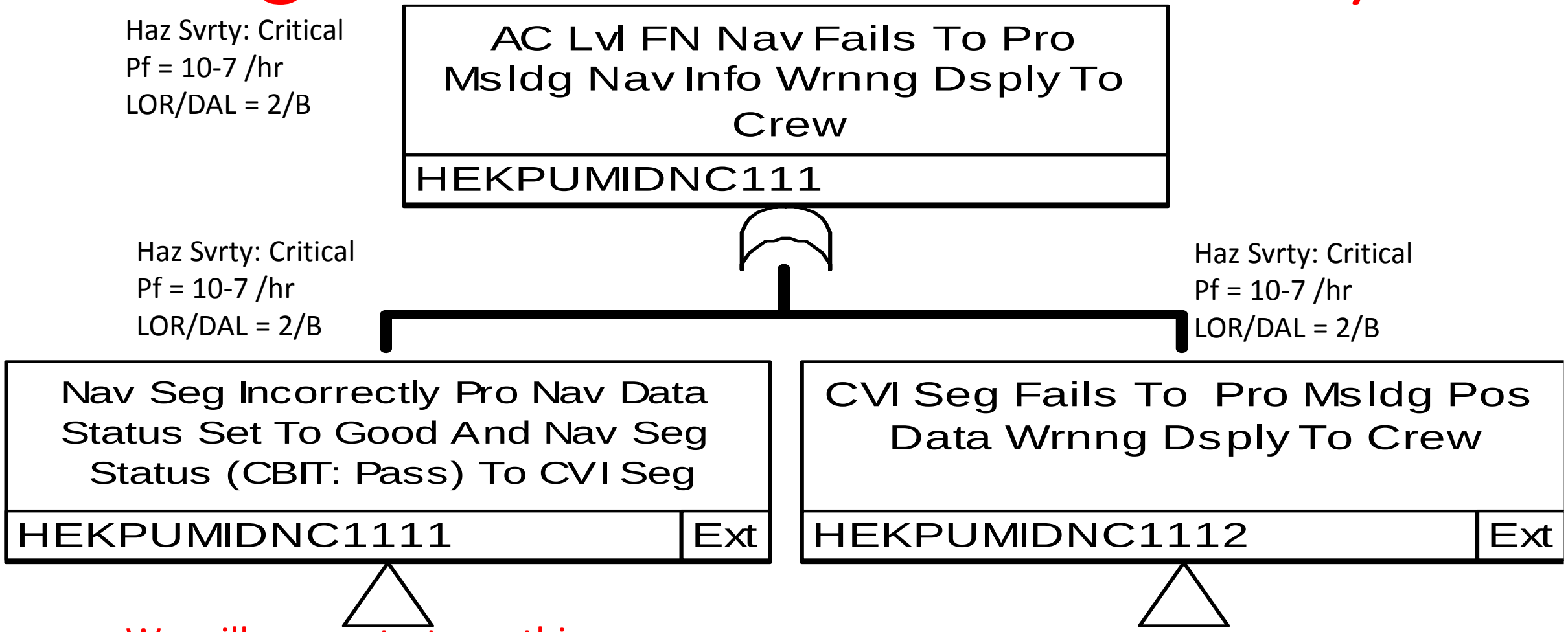
Aircraft-Level Function Level Of Design Functional Model



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



We will concentrate on this one

Segment Level Of Design

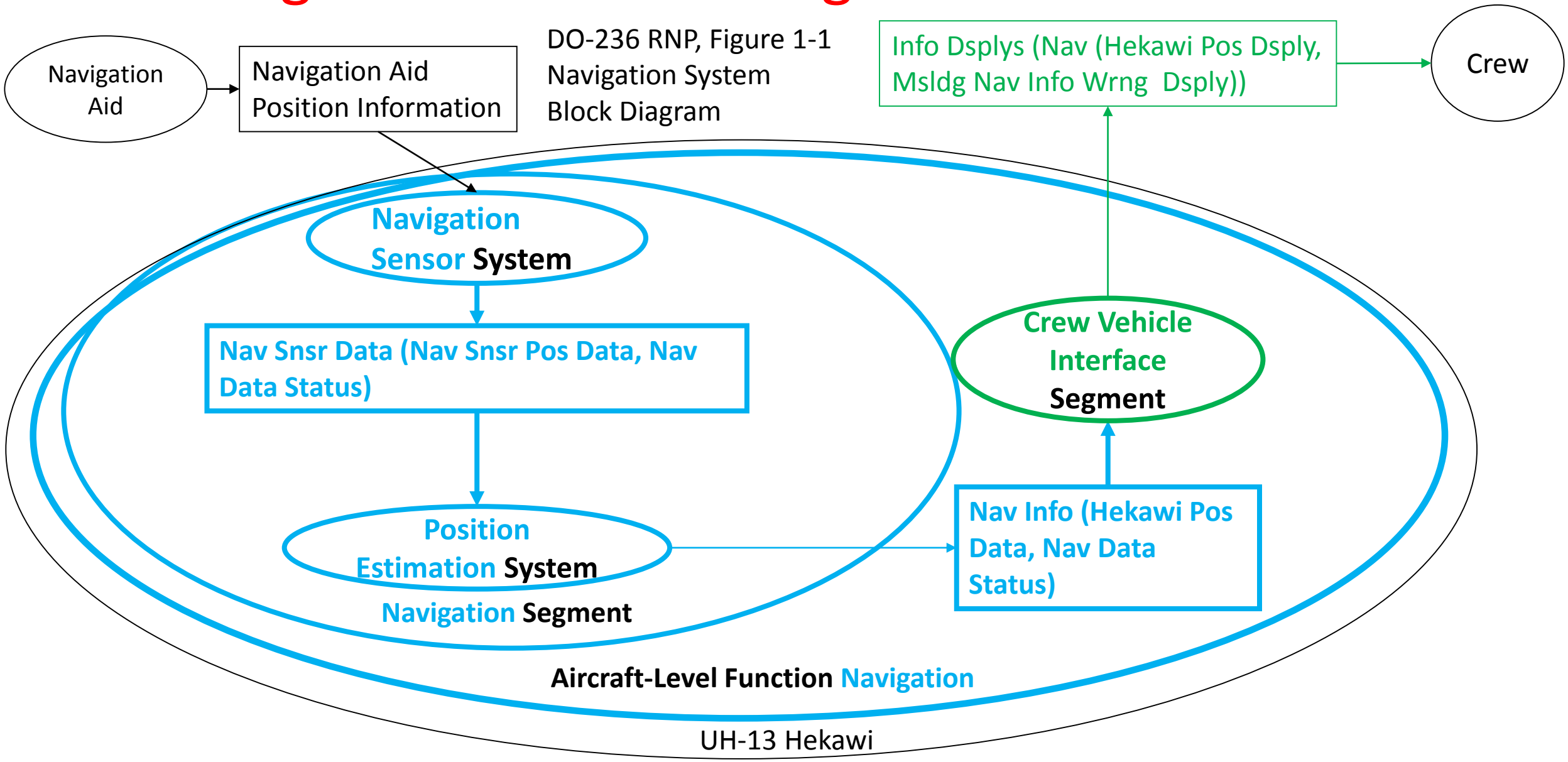
Aircraft – (UH-13 Hekawi) Composed of one or more:

Aircraft-Level Functions – (Navigation) Composed of one or more:

Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:

Systems – (Navigation Sensor System, …)

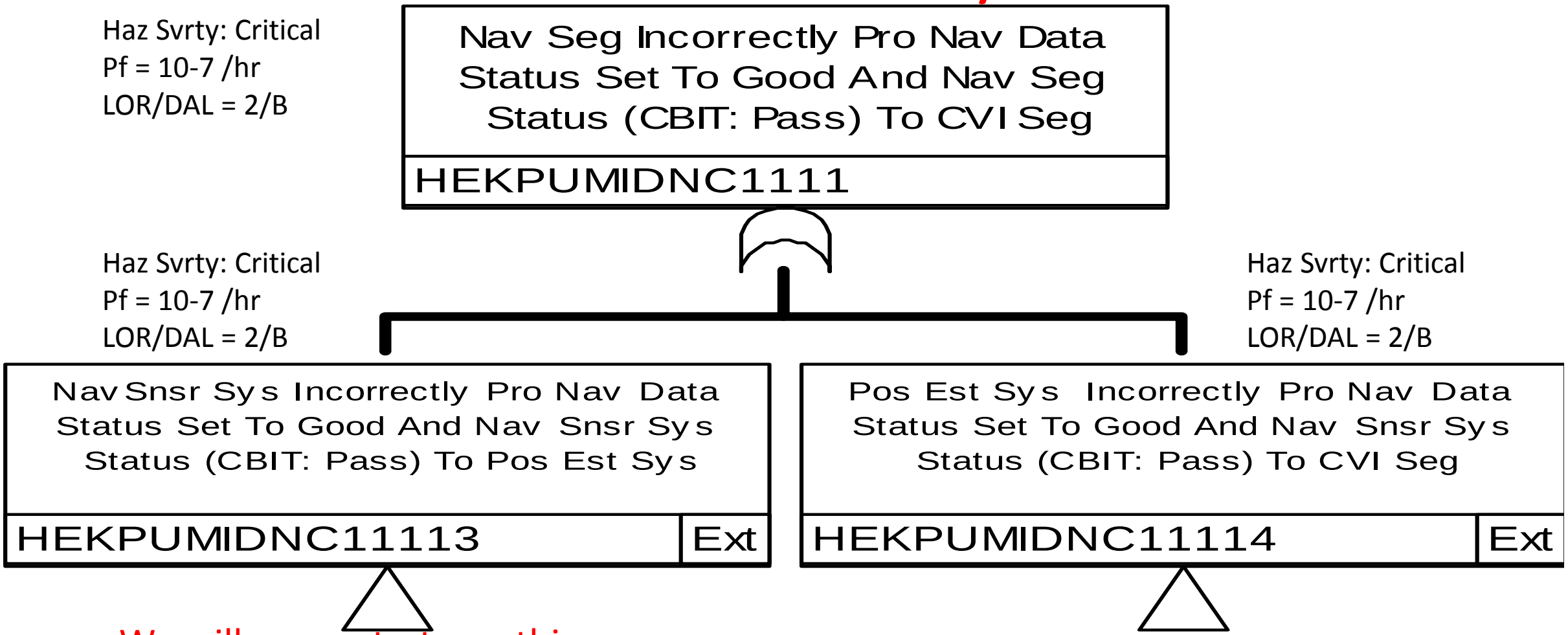
Segment Level Of Design Functional Model



ARP4761 Documentation Tie-In

- 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



We will concentrate on this one

System Level Of Design

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

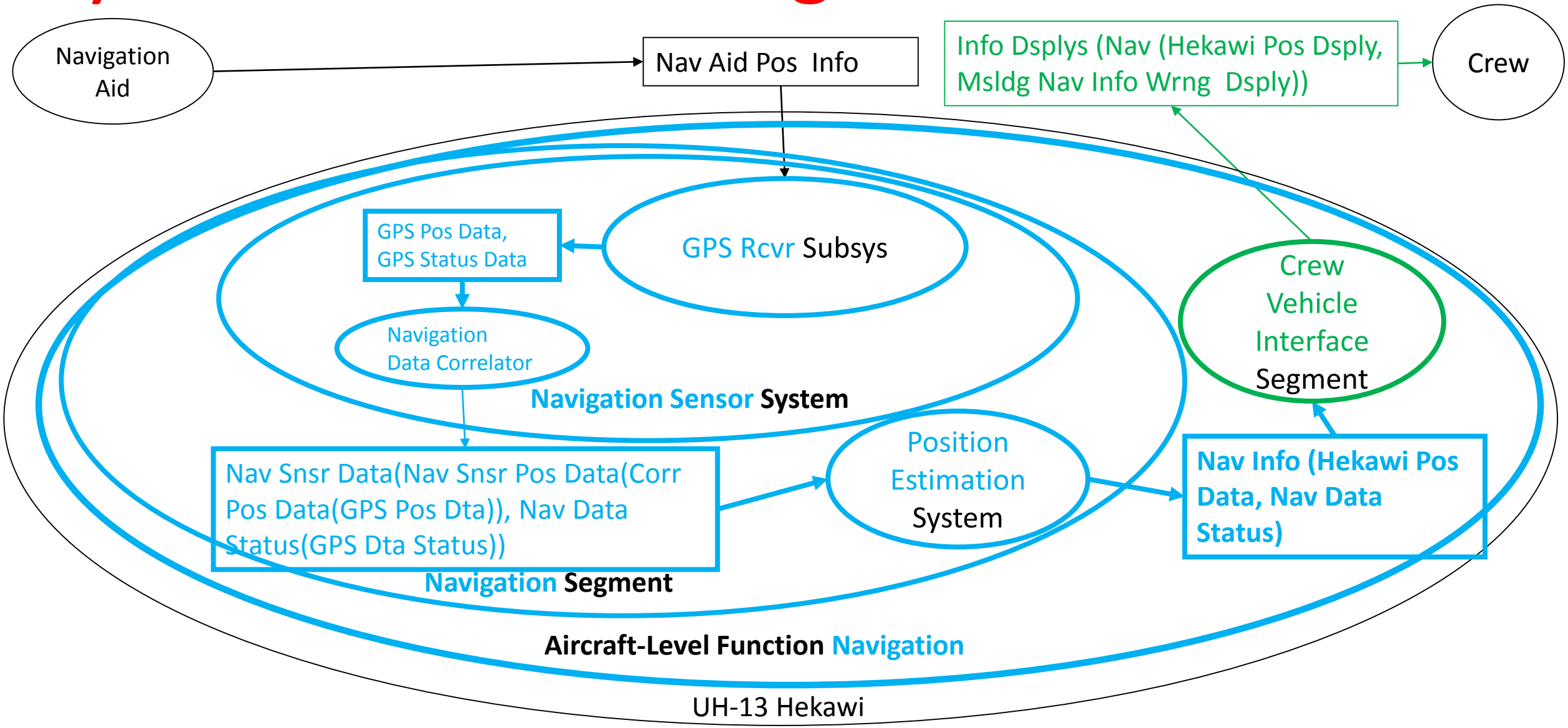
Aircraft-Level Functions – (Navigation) Composed of one or more:

Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:

Systems – (Navigation Sensor System, …) Composed of one or more:

Subsystems – (GPS Receiver Subsystem, …)

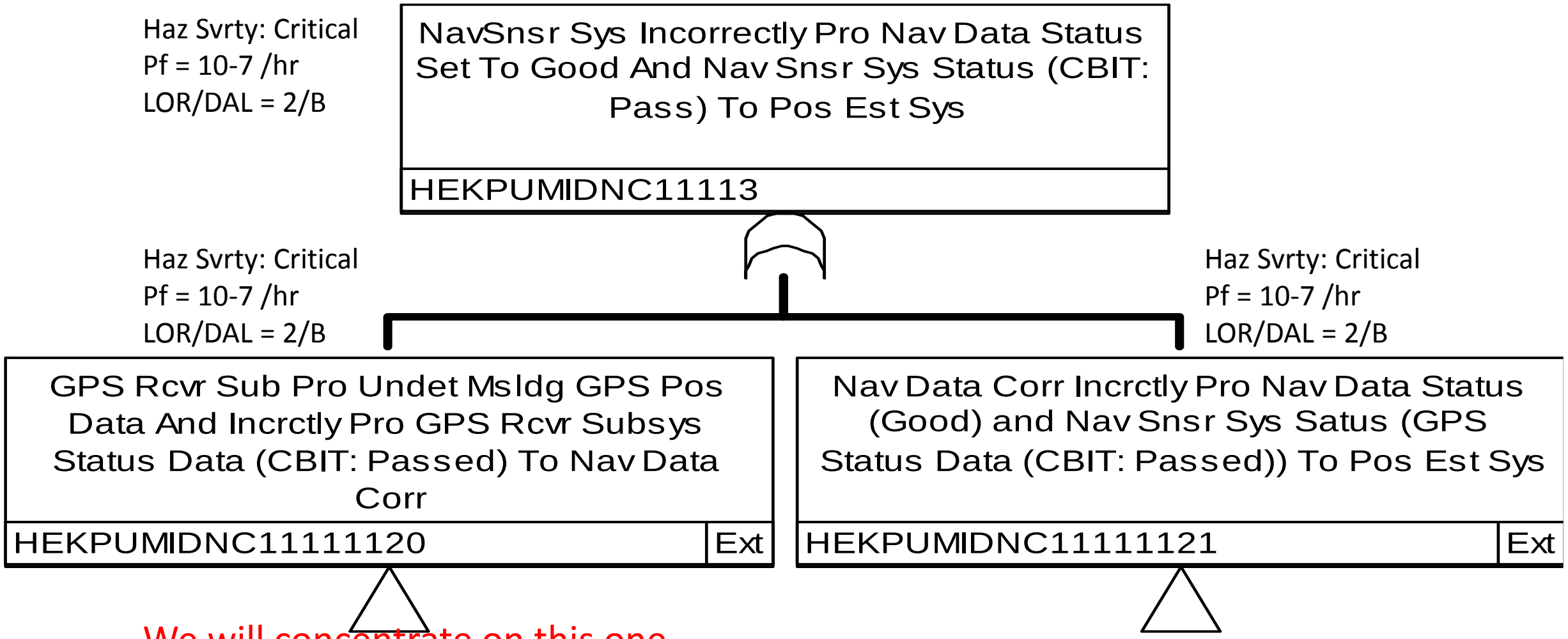
System Level Of Design Functional Model



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



We will concentrate on this one

Subsystem Level Of Design

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

Aircraft-Level Functions – (Navigation) Composed of one or more:

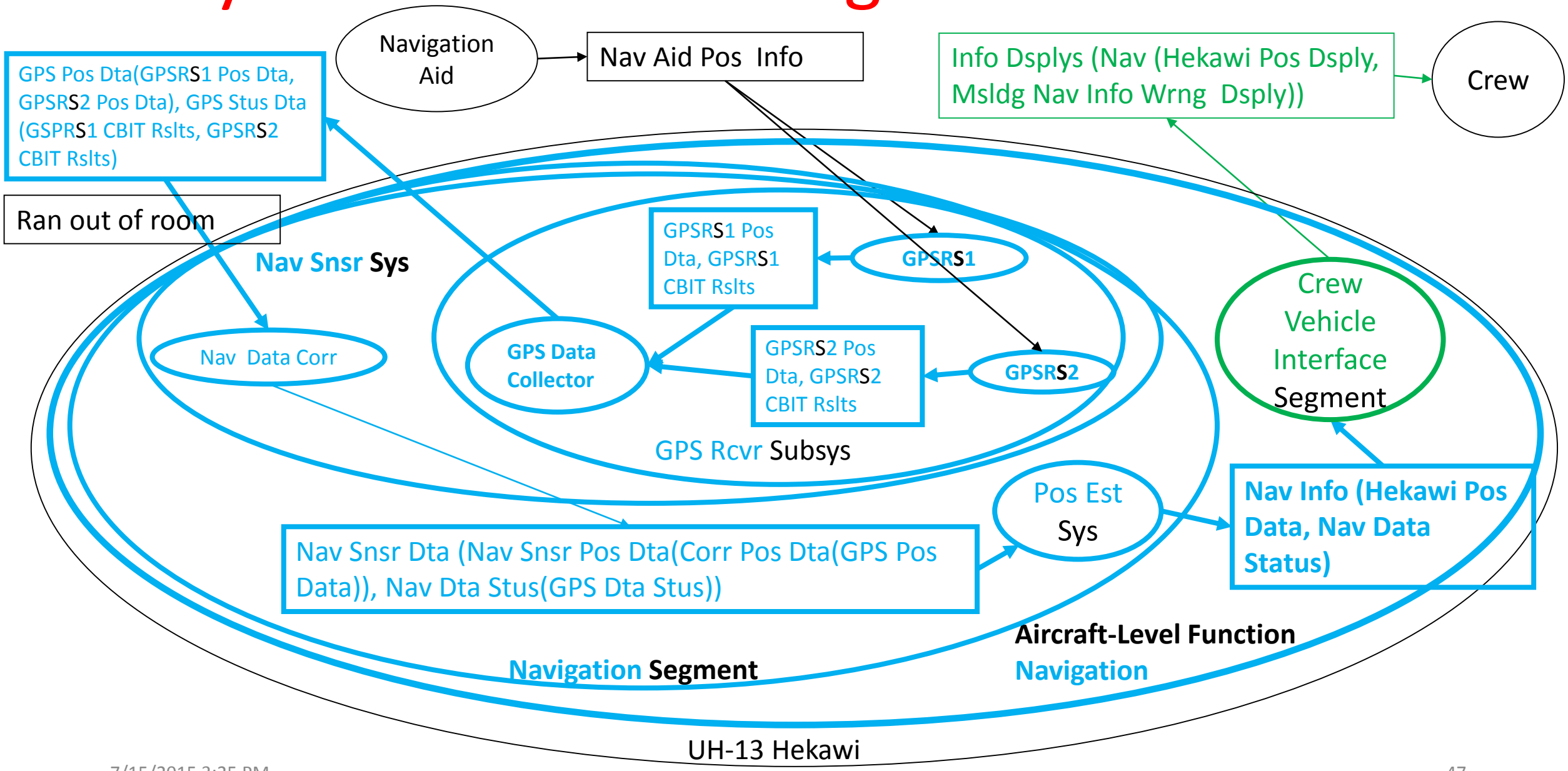
Segments – (Navigation, Crew Vehicle Interface) Composed of one or more:

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 Level Of Design Functional Model

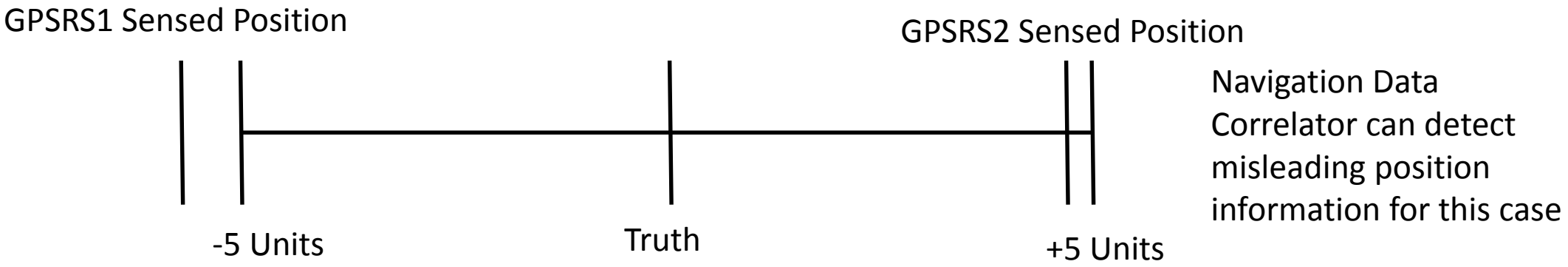


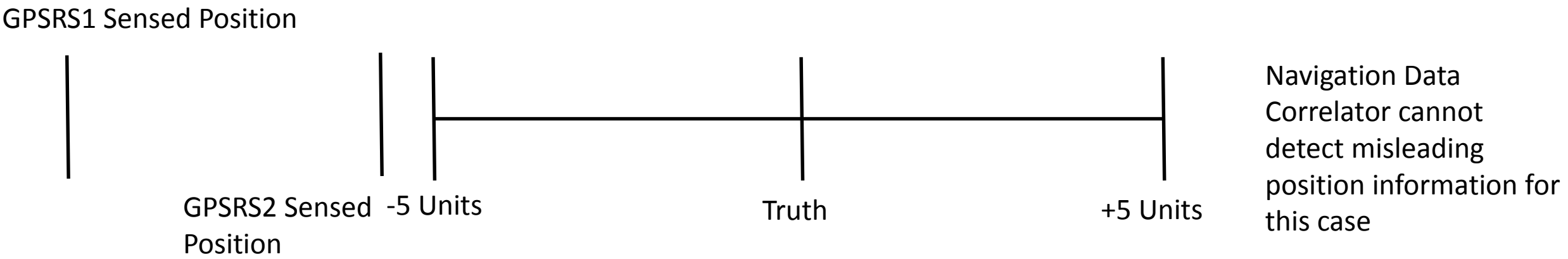
Misleading Information

- 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 |GPSRS1 Position Data - GPSRS2 Position Data| > 2* Tolerance



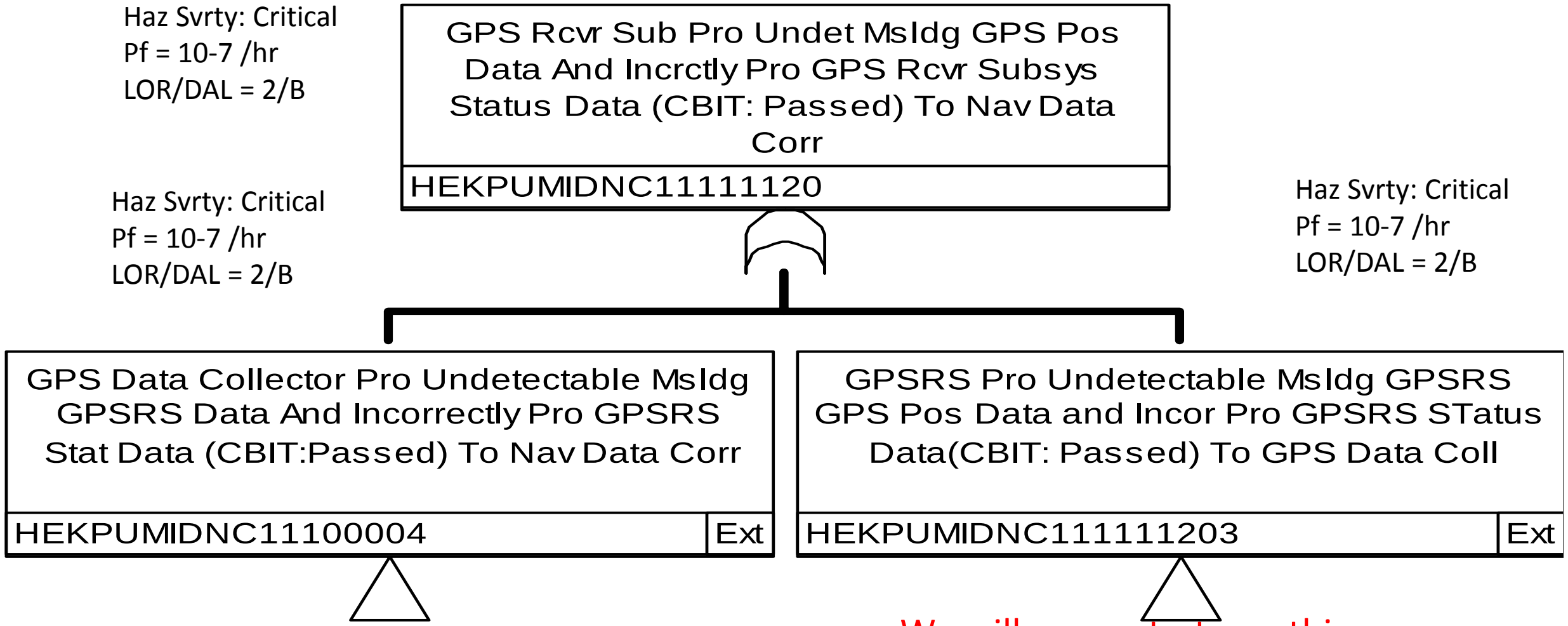


The best that we can actually do is provide the crew with absolute certainty that they are lost because we have no way of knowing which case we are dealing with!

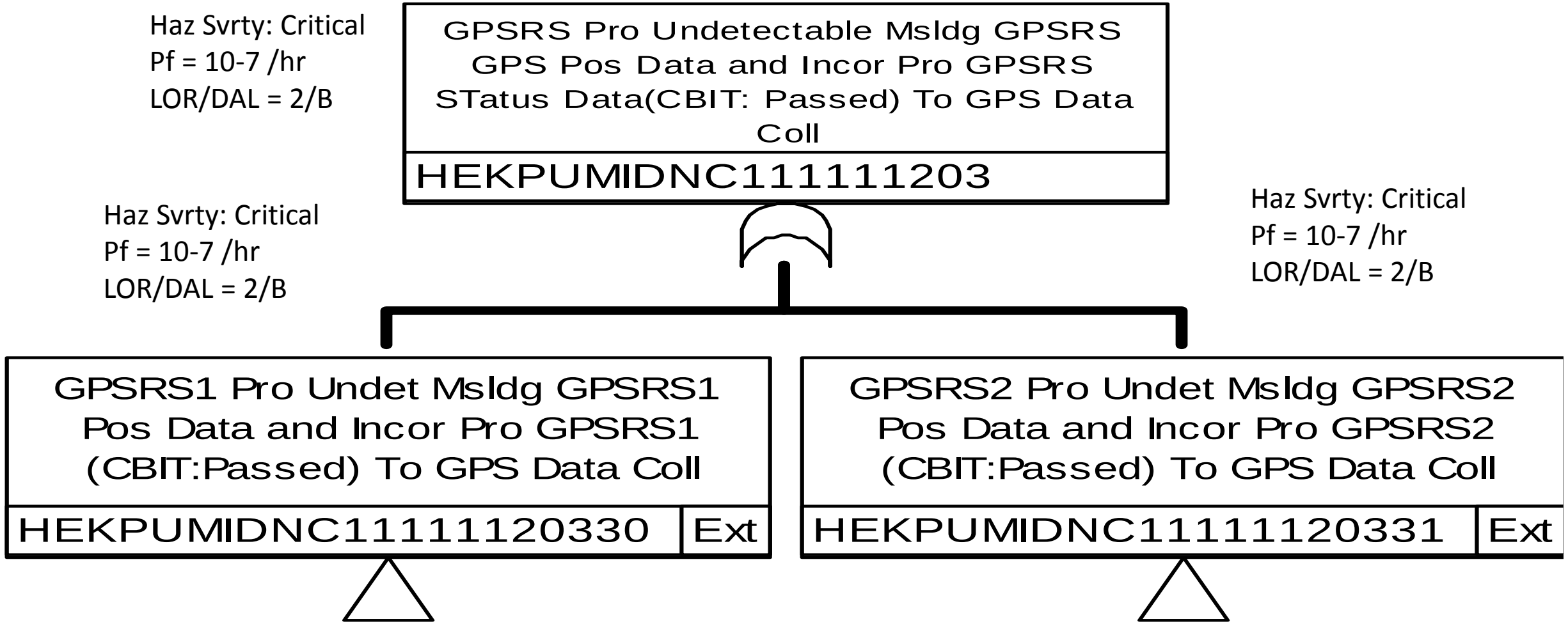
ARP4761 Documentation Tie-In

- 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

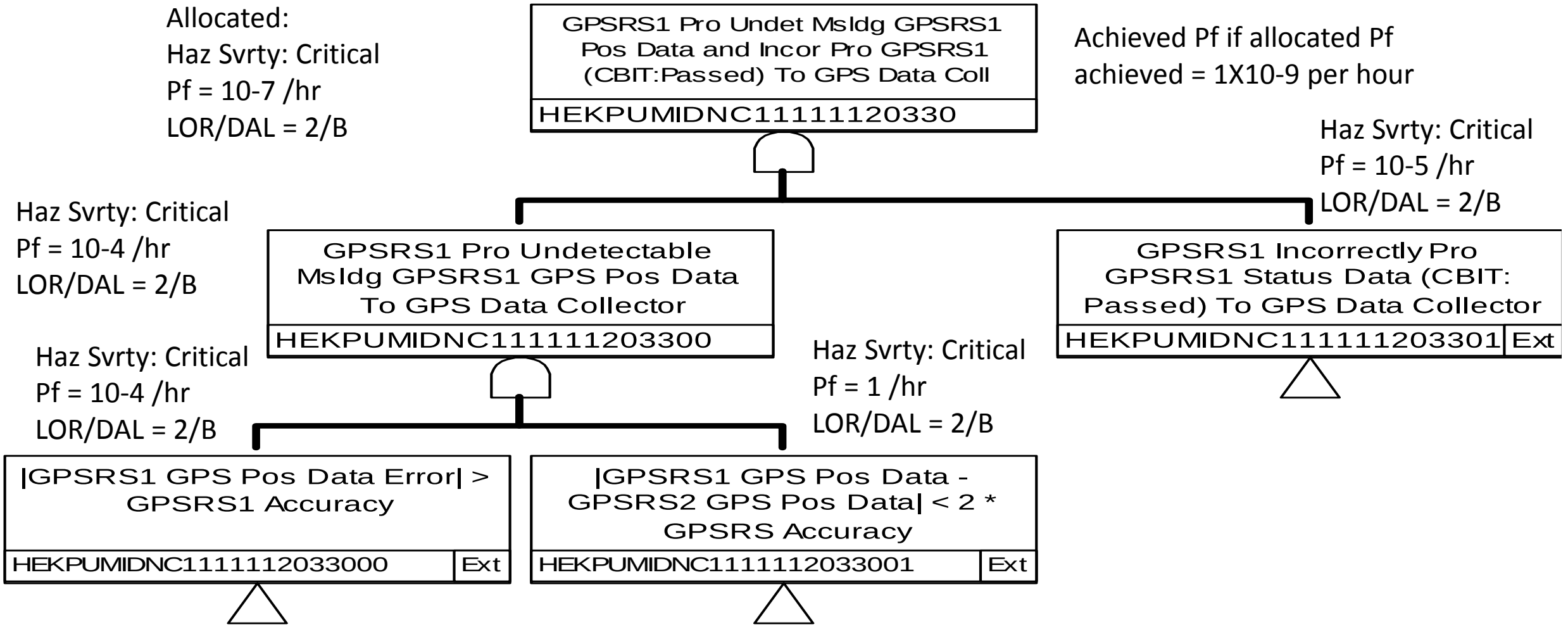
Subsystem Level Of Design Functional Model



Subsystem Level Of Design Functional Model



Subsystem Level Of Design Functional Model



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 (Pf = $1.0X10^{-5}$ 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* 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

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* Acme AG-72 GPS System position tolerance AND one or neither GPSRS1 CBIT Results and GPSRS2 CBIT Results are set to Failed
    - Then set GPS Data Status To Good
  - Else
    - Set GPS Data Status To Bad