Sample Intent Specification: Altitude Switch

Nancy G. Leveson

Massachusetts Institute of Technology
Safeware Engineering Corporation

Preface

The following example is taken from a specification by Steven Miller at Rockwell Collins of an altitude switch. His specification is part of a draft paper titled "Modeling Software Requirements for Embedded Systems." His methodology, however, is quite different from that being demonstrated in this document.

Contents

Level 1

System-Level Goals, Requirements, Constraints

Introduction

The Altitude Switch is a reusable component that turns power on to a Device of Interest (DOI) when the aircraft crosses a particular altitude. The first implementation will only turn power on when the aircraft descends below the altitude, but a switch that is activated upon ascent through the altitude may be required in the future and therefore it is included in the specification of levels 1 and 2 of this intent specification. This will allow the reuse of these levels for future product family members. The ASW receives altitude information from a variety of sensors and computes an estimate of the aircraft's true altitude. It then determines whether or not to power on the DOI.

This example problem was derived from a specification by Steve Miller at Rockwell-Collins. Minor changes have been made to better demonstrate the intent specification methodology. Because of the simplicity of the device, this intent specification is realtively trivial in some parts, particularly the desscription of the system design principles (Level 2). For a better example of the information found on this level, the reader is referred to our TCAS II Intent Specification.

Historical Perspective

The history of this device and its development is unknown to me.

Environment

There will be four types of devices in the environment with which the altitude switch must communicate. The actual types and number of each device can vary for each product in the family.

Device of Interest (DOI): The DOI may be any aircraft component that can receive an electronic signal to control its operation.

Environmental assumption:
[EA.1]
The DOI will be capable of providing information about its status (on or off) or there will be some other independent way to determine its status.

Watchdog Timer: A watchdog timer will be used to detect:

1. Failure of the altitude switch or
2. The inability of the altitude switch to determine the aircraft altitude within a given period of time

and to take action in those events.

Digital Altimeter(s): There may be one or more digital altimeters that report the aircraft altitude.

Analog Altimeter(s): There may be one or more analog altimeters that report the aircraft altitude.

Operator

[OP.1]
The pilot shall take appropriate action when the altitude switch fails.

[OP.2]
The pilot shall inhibit the operation of the altitude switch when ....

[OP.2]
The pilot shall reset the altitude switch when ....

Human Interface Requirements

[1.1]
There shall be a means for the pilot to inhibit the operation of the ASW.

[1.2]
There shall be a means for the pilot to reset the ASW.

[1.3]
The pilot shall be informed about any failure of the altitude switch.

Functional Goals

[G.1]
The altitude switch shall turn on a DOI when the aircraft decends below or ascends above (passes through) a threshold altitude ($\rightarrow$1.4, 1.5).

[G.2]
Failure of the ASW to perform its function shall be indicated to the pilot ($\rightarrow$1.6, 1.7, 1.8)

[G.3]
The pilot shall be able to inhibit the operation of the ASW ($\rightarrow$1.9, 1.10).

High-Level Functional Requirements

[1.4]
The ASW shall turn power on to a DOI when the aircraft ascends below or ascends above a threshold altitude (ALT) above ground level (G.1)(↓2.1).

> ASSUMPTION: The specification is to be reusable and describe a family of products and therefore the appropriate altitude (ALT) will be determined for each ASW implementation.

> [1.4.1]
> If the DOI is powered off after the aircraft descends below the altitude threshold, the ASW shall not reapply power to the DOI unless the aircraft again descends below the threshold altitude.
>
> > RATIONALE: This requirement provides hysteresis so the altitude switch is not continually powered on and off while the aircraft is flying at the threshold altitude.

[1.5]
The ASW shall receive altitude information from one or more sensors and compute an estimate of the aircraft's true altitude from this information (G.1) (↓2.2).

> ASSUMPTION: Each product will possibly have different numbers and types of altitude sensors.

[1.6]
The ASW shall detect a fault under the following conditions (G.2):

a. The DOI fails to turn on in a period of TIME-A after power is applied (↓2.??).

> ASSUMPTION: The time in which the device will have been determined to have failed after receiving a command to turn on will depend upon the device and the aircraft design and must be set for each product family member.

b. The altitude cannot be determined within a period of TIME-B from the last valid altitude determination (↓2.??).

c. An internal ASW failure is detected (↓2.??).

[1.7]
Detection of a fault shall be indicated by failure of the ASW to strobe a watchdog timer (G.2) (↓??).

> ASSUMPTION: Failure of the watchdog to be strobed within a deadline will result in separate hardware illuminating a fault indicator lamp in the cockpit.

[1.8]
The ASW shall assume its initial state when a reset signal is received (G.2) (↓2.??).

> ASSUMPTION: All previous information about altitude or faults obtained during the period when the ASW is inhibited will be discarded once the reset occurs. The reset will be used by the pilot to clear fault indications and try again.

[1.9]
If the ASW receives an inhibit signal, it shall not turn the device on nor indicate a fault (G.3) ↓2.??).

> ASSUMPTION: The inhibit will be used by the pilot to prevent the DOI from being turned on even though the altitude threshold has been crossed.

[1.10]
The inhibit condition shall remain on until the pilot turns it off (G.3) (↓2.??).

System Limitations

TBD

System Design Constraints

Non-Safety Related

[C1]
The altitude switch shall not apply power to the DOI if the DOI is already powered on.

> RATIONALE: I do not know the reason for this restriction.

[C2]
The ASW must operate independently from any operator action except for reset and inhibit.

> RATIONALE: The ASW function should not add to operator workload. In addition, failure to turn on the device should not be subject to operator error.

Safety Related

Because this is simply a component within a larger system, safety requirements cannot be determined. If the ASW is used to determine when to add air freshener to the cabin ventilation system before landing, then there are no safety-related constraints. If it is used to lower the landing gear, then it would be safety-critical and may have some specific constraints on its behavior. Safety-related constraints may need to be added and validated after a hazard analysis has been performed for the specific system in which the altitude switch is to be used.

Hazard Analysis

A hazard analysis cannot be performed without information about how the ASW will be used. For example, if turning on the DOI (or failing to do so) is hazard increasing, then the design might require all altitude-reporting devices to agree the threshold has been crossed. If the ASW output is hazard decreasing, then the design might require only one of the altimeters show the threshold has been crossed. Level 2 contains several optional designs (↓2.??) that can be linked to the hazard analysis when the environment in which the ASW is determined and a hazard analysis completed.

Because of this limitation, each member of the altitude switch product family will need to be evaluated for safety when the ASW usage and the specific environment in which it will be used is determined. This analysis may identify safety-related design constraints that must be enforced in the design.

Validation

No validation of these requirements has been done. If this were a real project, they would be reviewed by engineering, the potential customer, and perhaps marketing.

Level 2
System Design Principles

System Components—Environment

The external components will interface with the altitude switch in the following manner:

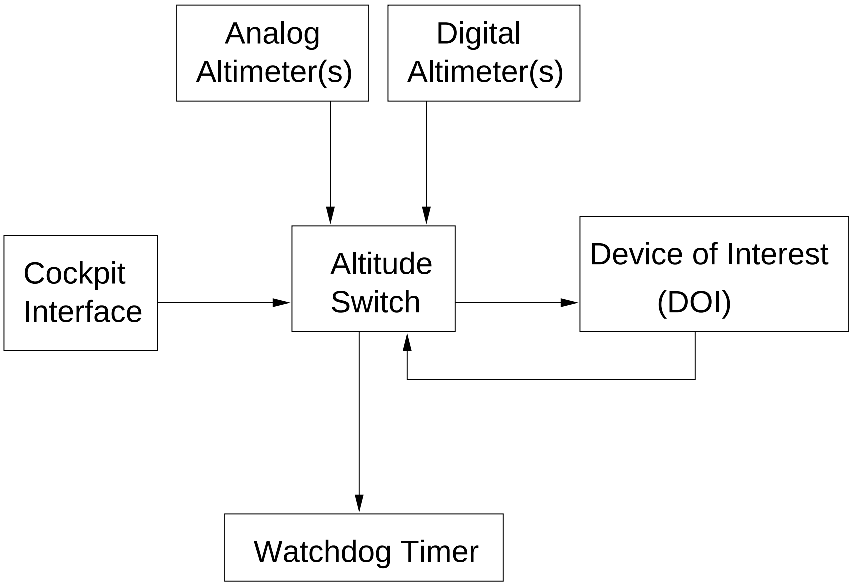


Figure 2.1: The ASW system components and environment

The analog altimeter value will range from 0 to 4000 feet AGL with a precision of 0.1 feet. However, due to the high cost and low reliability of A/D converters, the value will be sensed as a binary value (above or below the threshold).

If the digital altimeter value is outside its legitimate range, values above or below the minimum and maximum values, respectively will be mapped into the respective minimum or maximum and treated as valid values.

ASSUMPTION: The reason for this decision should be provided here.

ASW Logic

Altitude Determination

[2.1]
The decision to power on the DOI will be based on an estimate of the aircraft's true altitude (↑1.4).

> Assumption: The aircraft will always have a single true altitude and the environment of the altitude switch will have the capability to provide the information necessary to obtain a reasonable estimate of that altitude.

[2.2]
The algorithm for determining the altitude is likely to change, depending on the safety analysis. Four alternative agorithms are provided here and may be implemented in different products, depending on the specific use of the ASW (↑1.5). The initial product will use the lowest valid altitude.

[2.2.1]
Lowest Valid Altitude: The altitude is taken as the lowest valid altitude reported (↓3.altitude). If no valid altitude is available, the altitude will be assumed to be undeterminable.

> Assumption: This algorithm will be used when the ASW is used to indicate that the aircraft has descended below a threshold altitude. The use of this algorithm is most appropriate when (1) reliability is more important than safety (the action of turning on the DOI is not safety-related) *or* (2) turning on the DOI is a safety-increasing action for the aircraft as a whole.

[2.2.2]
Highest Valid Altitude: The altitude is taken as the highest valid

altitude reported (↓*Not implemented in current product*). If no valid altitude is reported, the altitude will be assumed to be undeterminable.

> Assumption: This algorithm will be used when the ASW is used to indicate that the aircraft has ascended above a threshold altitude. The use of this algorithm is most appropriate when reliability is more important than safety (the action of turning on the DOI is not safety-related) or turning on the DOI is a safety-increasing action for the aircraft as a whole.

[2.2.3]
Majority Valid Altitude: Whether the aircraft is below or above the threshold will be determined by a majority vote of the valid altitudes reported. If there is no majority, then the altitude will be assumed to be indeterminate (↓*Not implemented in current product*).

> Assumption: This algorithm could be used for either ascending above or descending below a threshold altitude. The use of this algorithm is most appropriate when turning on the DOI is safety-decreasing and inadvertent operation of the DOI is unsafe.

[2.2.4]
Most Conservative Algorithm: The altitude will be determinable only if all altimeters agreed that the aircraft is below or above the threshold altitude. There must be at least N valid altitudes reported or the altitude is treated as indeterminate (↓*Not implemented in current product*).

> Assumption: This algorithm will be used under the conditions that the operation of the ASW and turning on the DOI is safety-decreasing and that turning on the DOI under the wrong conditions could endanger the continued safe flight of the aircraft. In this case, safety is more important than reliability.

[2.3]
Reported altitude information will be considered to be obsolete after AGE seconds (↑1.6).

Turning on the DOI

The power-on signal should remain on once the aircraft passes through the threshold until the ASW receives an indication that the DOI that it has turned on, even if the aircraft crosses the threshold again.

ASSUMPTION: This requirement provides hysteresis so that the DOI is not continually turned on and off if the aircraft flies right at the threshold altitude.

Fault Detection

[2.4]
Three types of faults shall be detected (↑1.6): an internal fault, the failure of the DOI to turn on, and the failure of the altimeters.

[2.4.5]
Internal failures refers to internal hardware faults. The faults to be detected will be determined by the engineers.

[2.4.6]
Detected faults will be reported by failing to strobe the watchdog timer (↑1.7).

Inhibiting and Resetting ASW Operation

Inhibit (↑1.9)

[2.5]
When the inhibit is on, the ASW shall not issue any commands to power on the DOI.

[2.6]
When the inhibit is on, the ASW shall not indicate a fault.

[2.7]
All other ASW functions shall be unaffected by the inhibit signal.

Reset (↑1.8)

[2.8]
The reset signal shall return the ASW to its initial state.

[2.9]
If the ASW operation is inhibited when the reset signal is received, the ASW shall be returned to its initial state but the inhibit on operation will remain until the pilot cancels it.

RATIONALE: There may be reasons for the pilot to reset the ASW while still wanting its operation to be inhibited. If the reset causes an indirect mode transition from inhibited to not inhibited, there is a possibility for mode confusion (the pilot thinks operation is inhibited when it is not). To avoid this possibility, the pilot must explicitly turn off the inhibit independently from the reset switch.

Pilot–ASW Interface

Controls

The reset and inhibit controls are independent (→2.x). When the inhibit is removed, the state of the ASW is affected only in so much as reporting faults and turning on the DOI is again allowed.

A reset does not affect the status of the inhibit, which will remain in the state in which it was when the reset is pushed.

Displays

A fault indicator light will illuminate when a fault is detected. Responsibility for turning this light on and off lies outside the altitude switch.

Pilot Tasks and Procedures

Reset and inhibit are independent. To turn off the inhibit, the pilot must push the inhibit. Reset will not reverse the inhibit.

Verification and Validation

The simplicity of the algorithms may preclude the need for rigorous scientific validation at this level.

Verification: Test plan System test must include ...

Level 3
Blackbox Behavior

Communication and Interfaces

Input messages to the ASW contain the altitude and status from an Analog Radio Altimeter, the alitude and status from two Digital Radio Altimeters, inhibit and reset signals, and the DOI status.

One output message contains a power-on signal to the DOI and a second output message results in the strobing of a watchdog timer.

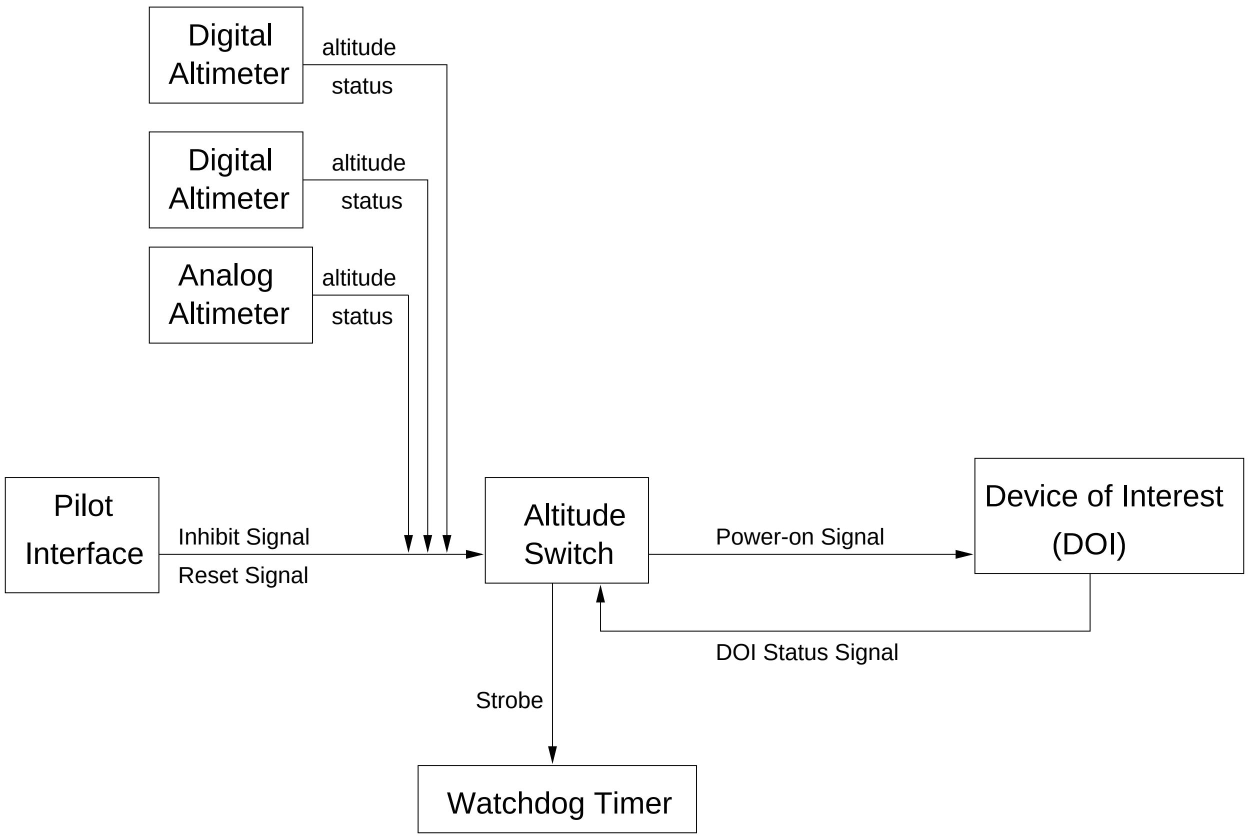


Figure 2.2: Communication Between Components

Message Contents

Digital Altimeter →ASW:

1. **Status signal** denoting whether the altitude data has failed, does not exist, is normal, or is test data.
2. **Altitude Data:** Range will be from -20 to 2500 feet AGL with a precision of 0.1 feet. Values below -20 will be treated as an altitude valid value of -20 feet and those above 2500 will be treated as a value of 2500 feet.

Analog Altimeter →ASW:

1. **status signal** denoting whether the analog altitude data is *valid* or *invalid* (↑2.??? ↓4.???).
2. **Altitude Data** will have a value denoting that the aircraft is *above* or *below* the threshold. (↑2.??, ↓4.??).

Cockpit Interface →ASW

1. Inhibit signal (on or off)
2. Reset signal (T or F)

DOI →ASW: status signal (on or off)

ASW →DOE: Power-on command

ASW→Watchdog Timer: Strobe

Flightcrew Behavioral Requirements

This section would contain the pilot tasks and procedures. These might be specified using SpecTRM-RL operational task models.

Pilot-ASW Interface

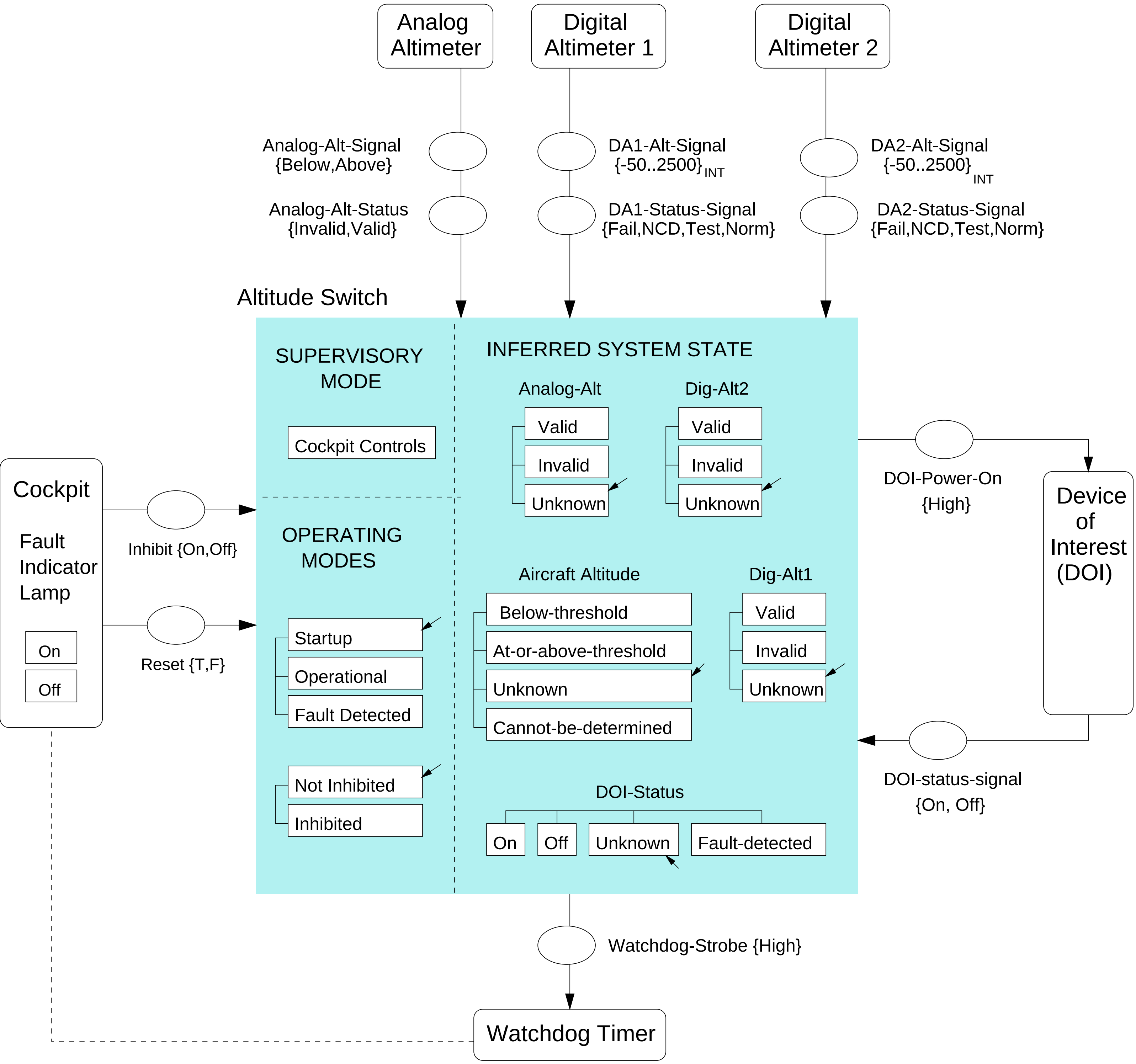
Controls

The pilot shall have a reset switch and an inhibit button. The inhibit button will light up to indicate that the ASW has been inhibited.

Displays

A fault indicator lamp will light in the cockpit to indicate that the watchdog timer has timed out and a fault has occurred in the altitude switch.

ASW Blackbox Behavior


Analog Altimeter
Digital Altimeter 1
Digital Altimeter 2
Analog-Alt-Signal {Below,Above}
Analog-Alt-Status {Invalid,Valid}
DA1-Alt-Signal {-50..2500} INT
DA1-Status-Signal {Fail,NCD,Test,Norm}
DA2-Alt-Signal {-50..2500} INT
DA2-Status-Signal {Fail,NCD,Test,Norm}
Altitude Switch
SUPERVISORY MODE
Cockpit Controls
OPERATING MODES
Startup
Operational
Fault Detected
Not Inhibited
Inhibited
INFERRED SYSTEM STATE
Analog-Alt
Valid
Invalid
Unknown
Dig-Alt2
Valid
Invalid
Unknown
Aircraft Altitude
Below-threshold
At-or-above-threshold
Unknown
Cannot-be-determined
Dig-Alt1
Valid
Invalid
Unknown
DOI-Status
On
Off
Unknown
Fault-detected
Cockpit
Fault Indicator Lamp
On
Off
Inhibit {On,Off}
Reset {T,F}
DOI-Power-On {High}
Device of Interest (DOI)
DOI-status-signal {On, Off}
Watchdog-Strobe {High}
Watchdog Timer

Output Command

DOI-Power-On

Destination: DOI

Acceptable Values: {high}

Initiation Delay: 0 milliseconds

Completion Deadline: 50 milliseconds

Exception-Handling: (What to do if cannot issue command within deadline time)

Feedback Information:

Variables: DOI-status-signal

Values: high (on)

Relationship: Should be on if ASW sent signal to turn on

Min. time (latency): 2 seconds

Max. time: 4 seconds

Exception Handling: DOI-Status changed to Fault-Detected

Reversed By: Turned off by some other component or components. Do not know which ones.

Comments: I am assuming that if we do not know if the DOI is on, it is better to turn it on again, i.e., that the reason for the restriction is simply hysteresis and not possible damage to the device.

This product in the family will turn on the DOE only when the aircraft descends below the threshold altitude. Only this page needs to change for a product in the family that is triggered by rising above the threshold.

References: ↑ ↓

CONTENTS

= discrete signal on line PWR set to high

TRIGGERING CONDITION

Operating Mode	Operational	T
	Not Inhibited	T
State Values	DOI-Status = On	F
	Altitude = Below-threshhold	T
	Prev(Altitude) = At-or-above-threshold	T

Output Command

Watchdog-Strobe

Destination: Watchdog Timer

Acceptable Values: high signal (on)

Min-Time-Between-Outputs: 0

Max-Time-Between-Outputs: 200_{PERIOD} msec

Exception-Handling:

Feedback Information: None

Reversed By: Not necessary

Comments:

References:

CONTENTS

= High signal on line WDT

TRIGGERING CONDITION

Operating Mode	Operational	T		
	Startup		T	
	Inhibited			T
State Values	Time <= (Time sent Watchdog Strobe) + 200 msec	T		T
	DOI-Status = Fault-detected	F		
	Time >= (Time entered Altitude.Cannot-be-determined) + 2_{DL} secs.	F		

Operating Mode

ASW

Description:

Comments: No information about how an internal fault is detected, what types detected, etc.

References:

Appears in: DOI-power-on, Watchdog-strobe

DEFINITION

= Startup

Powerup	T

= Operational

Controls.Reset = T	T			
Startup		T	T	T
Analog-Alt = Valid		T		
Dig-Alt1 = Valid			T	
Dig-Alt2 = Valid				T

= Internal-Fault-Detected

Internal-fault -detected	T	
Startup		T
Time >= Time entered Startup + 3 secs		T

.

State Value

DOI-Status

Obsolescence: 2 seconds

Exception-Handling: Goes into unknown state

Description:

Comments: There is nothing in the requirements that says what to do if a power-off message is sent and no status message is received from the DOI within 2 seconds. I decided it was safest to have this indicate a possible fault so the watchdog will time out and light the fault indicator lamp in the cockpit.

References:

Appears in: DOI-Power-On, Watchdog-Strobe

DEFINITION

= On

DOI-status-signal = On	T

= Off

DOI-status-signal = Off	T

= Unknown

Powerup	T		
Controls.Reset = T		T	
DOI-status-signal = obsolete			T

= Fault-Detected

Time >= (Time sent DOI-Power-On Message) + 2 seconds	T	T
DOI-status-signal = Off	T	
Time > Time received DOI-status-signal + 2 seconds		T

Column 1: Sent power on message but DOI did not turn on
Column 2: Sent power on message but never got feedback

State Value

Altitude

Obsolescence: 2 seconds

Exception-Handling: Because the altitude-status-signals change to obsolete after 2 seconds, altitude will change to Unknown if all input signals are lost for 2 seconds.

Description:

Comments:

References:

Appears in: DOI-Power-On

DEFINITION

= Unknown

Powerup	T		
Controls.Reset		T	
Analog-ALT = Unknown			T
Dig-Alt1 = Unknown			T
Dig-Alt2 = Unknown			T

= Below-threshold

Analog-Valid-and-Below	T		
Dig1-Valid-and-Below		T	
Dig2-Valid-and-Below			T

= At-or-above-threshold

Analog-Valid-and-Above	T	T	T	F	T	F	F
Dig1-Valid-and-Above	T	T	F	T	F	T	F
Dig2-Valid-and-Above	T	F	T	T	F	F	T

= Cannot-be-determined

Analog-Alt = Invalid	T
Dig-Alt1 = Invalid	T
Dig-Alt2 = Invalid	T

State Value

Analog-Alt

Obsolescence: 2 seconds

Exception-Handling: Will change to unknown when analog-alt-signal becomes obsolete (more than 2 seconds elapse since last message from Analog Altimeter)

Description:

Comments:

References:

Appears in: Altitude

DEFINITION

= Valid

Analog-Alt-Status = Valid	T

= Invalid

Analog-Alt-Status = Invalid	T

= Unknown

Analog-Alt-Status = Obsolete	T		
Powerup		T	
Controls.Reset = T			T

.

State Value

Dig-Alt1

Obsolescence: 2 seconds

Exception-Handling: Will change to unknown when DA1-Status-Signal becomes obsolete (more than two seconds elapse since last mesage from Digital Altimeter 1).

Description:

Comments:

References:

Appears in: Altitude

DEFINITION

= Valid

DA1-Status-Signal = Norm	T

= Invalid

DA1-Status-Signal = {Fail, NCD, Test}	T

= Unknown

DA1-Status-Signal = Obsolete	T		
Powerup		T	
Controls.Reset = T			T

State Value

Dig-Alt2

Obsolescence: 2 seconds

Exception-Handling: Will change to unknown when DA2-Status-Signal becomes obsolete (more than two seconds elapse since last mesage from Digital Altimeter 2).

Description:

Comments:

References:

Appears in: Altitude

DEFINITION

= Valid

DA2-Status-Signal = Norm	T

= Invalid

DA2-Status-Signal = {Fail, NCD, Test}	T

= Unknown

DA2-Status-Signal = Obsolete	T		
Powerup		T	
Controls.Reset = T			T

.

Input Value

DOI-Status-Signal

Source: DOI

Type: Enumerated

Possible Values (Expected Range): {On, Off}

Exception-Handling:

Arrival Rate (Load): ??

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: 2 seconds

Exception-Handling: Assumes value Obsolete

Description:

Comments:

References:

Appears in: DOI-status

DEFINITION

= FIELD (Status in DOI-Status-Message)

Receive DOI-Status-Message FROM DOI	T

= PREV (DOI-Status-Signal)

Receive DOI-Status-Message FROM DOI	F
Time <= Time (DOI-Status-Message arrived) + 2 seconds	T

= Obsolete

Receive DOI-Status-Message FROM DOI	F	
Time > Time (DOI-Status-Message arrived) + 2 seconds	T	
Powerup		T

Input Value

Analog-Alt-Status

Source: Analog Altimeter

Type: Enumerated

Possible Values (Expected Range): {Invalid, Valid}

Exception-Handling:

Arrival Rate (Load): ??

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: 2 seconds

Exception-Handling: Assumes value Obsolete

Description:

Comments:

References:

Appears in: Analog-Alt

DEFINITION

= FIELD (Status in Analog-Alt-Message)

Receive Analog-Alt-Message FROM Analog-Altimeter	T

= PREV (Analog-Alt-Status)

Receive Analog-Alt-Message FROM Analog-Altimeter	F
Time <= Time (Analog-Alt-Message arrived) + 2 seconds	T

= Obsolete

Receive Analog-Alt-Message FROM Analog-Altimeter	F	
Time > Time (Analog-Alt-Message arrived) + 2 seconds	T	
Startup		T

Input Value

Analog-Alt-Signal

Source: Analog Altimeter

Type: Enumerated

Possible Values (Expected Range): {Above, Below}

Exception-Handling:

Arrival Rate (Load): ??

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: 2 seconds

Exception-Handling: Assumes value Obsolete

Description:

Comments:

References:

Appears in: Altitude

DEFINITION

= FIELD (Altitude in Analog-Alt-Message)

Receive Analog-Alt-Message FROM Analog-Altimeter	T

= PREV (Analog-Alt-Signal)

Receive Analog-Alt-Message FROM Analog-Altimeter	F
Time <= Time (Analog-Alt-Message arrived) + 2 seconds	T

= Obsolete

Receive Analog-Alt-Message FROM Analog-Altimeter	F	
Time > Time (Analog-Alt-Message arrived) + 2 seconds	T	
Powerup		T

Input Value

DA1-Status-Signal

Source: Digital Altimeter 1

Type: Enumerated

Possible Values (Expected Range): {Fail, NCD, Test, Norm}

Exception-Handling:

Arrival Rate (Load): ??

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence:2 seconds

Exception-Handling: Assumes value Obsolete

Description:

Comments: Four possible values can be sent signifying Failure Warning, No Computed Data, Functional Test, and Normal Operation.

References:

Appears in: Dig-Alt1

DEFINITION

= FIELD (Status in DA1-Message)

Receive DA1-Message FROM Digital-Altimeter-1	T

= PREV (DA1-Status-Signal)

Receive DA1-Message FROM Digital-Altimeter-1	F
Time <= Time (DA1-Message arrived) + 2 seconds	T

= Obsolete

Receive DA1-Message FROM Digital-Altimeter-1	F	
Time > Time (DA1-Message arrived) + 2 seconds	T	
Powerup		T

Input Value

DA1-Alt-Signal

Source: Digital Altimeter 1

Type: integer

Possible Values (Expected Range): -20..2500

Exception-Handling: Values below -20 are treated as -20 and values above 2500 as 2500

Units: ??

Granularity: ??

Arrival Rate (Load): ??

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: 2 seconds

Exception-Handling:

Description:

Comments:

References:

Appears in: Altitude

DEFINITION

= FIELD (Altitude in DA1-Message)

Receive DA1-Message FROM Digital-altimeter-1	T

= PREV (DA1-Alt-Signal)

Receive DA1-Message FROM Digital-altimeter-1	F

= Obsolete

Receive DA1-Message FROM Digital-Altimeter-1	F	
Time > Time (DA1-Message arrived) + 2 seconds	T	
Powerup		T

Input Value

DA2-Status-Signal

Source: Digital Altimeter 1

Type: Enumerated

Possible Values (Expected Range): {Fail, NCD, Test, Norm}

Exception-Handling:

Arrival Rate (Load): ??

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: 2 seconds

Exception-Handling: Assumes value Obsolete

Description:

Comments: Four possible values can be sent signifying Failure Warning, No Computed Data, Functional Test, and Normal Operation.

References:

Appears in: Dig-Alt2

DEFINITION

= FIELD (Status in DA2-Message)

Receive DA2-Message FROM Digital-Altimeter-2	T

= PREV (Dig2-Status-Signal)

Receive DA2-Message FROM Digital-Altimeter-2	F
Time <= Time (DA2-Message arrived) + 2 seconds	T

= Obsolete

Receive DA2-Message FROM Digital-Altimeter-2	F	
Time > Time (DA2-Message arrived) + 2 seconds	T	
Powerup		T

Input Value

DA2-Alt-Signal

Source: Digital Altimeter 2

Type: integer

Possible Values (Expected Range): -20..2500

Exception-Handling: Values below -20 are treated as -20 and values above 2500 as 2500

Units: ??

Granularity: ??

Arrival Rate (Load): ??

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: 2 seconds

Exception-Handling:

Description:

Comments:

References:

Appears in: Altitude

DEFINITION

= FIELD (Altitude in DA2-Message)

Receive DA2-Message FROM Digital-altimeter-2	T

= PREV (DA2-Alt-Signal)

Receive DA2-Message FROM Digital-altimeter-2	F

= Obsolete

Receive DA2-Message FROM Digital-Altimeter-2	F	
Time > Time (DA2-Message arrived) + 2 seconds	T	
Powerup		T

Control Input

Inhibit

Source: Cockpit Inibit Button

Type: Enumerated

Possible Values (Expected Range): {on, off}

Arrival Rate (Load):

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: None

Description:

Comments:

References:

Appears in: ASW

DEFINITION

= FIELD (Value in Inhibit-Message)

Receive Inhibit-Message from Cockpit	T

= PREV (Inhibit)

Receive Inhibit-Message from Cockpit	F

= Obsolete

Powerup	T

Control Input

Reset

Source: Cockpit Reset Button

Type: Signal

Possible Values (Expected Range): {High}

Arrival Rate (Load):

Min-Time-Between-Inputs:
Max-Time-Between-Inputs:

Obsolescence: Not applicable (lasts only one step)

Description:

Comments:

References:

Appears in: Analog-Alt, DOI-Status, Altitude, Analog.Alt, Dig-Alt1, Dig-Alt2, ASW

DEFINITION

= True

Receive Inhibit Signal	T

= False

Prev (Reset) = True	T	
Powerup		T

Macro

Analog-Valid-and-Below

Description:

Comments:

References:

Appears in: Altitude2

DEFINITION

Analog-alt = Valid	T
Analog-Alt-Signal = below	T

Macro

Analog-Valid-and-Above

Description:

Comments:

References:

Appears in: Altitude2

DEFINITION

Analog-alt = Valid	T
Analog-Alt-Signal = above	T

Macro

Dig1-Valid-and-Below

Description:

Comments:

References:

Appears in: Altitude2

DEFINITION

Dig1-alt = Valid	T
DA1-Alt-Signal < 2000_{THRES}	T

Macro

Dig1-Valid-and-Above

Description:

Comments:

References:

Appears in: Altitude2

DEFINITION

Dig-Alt1 = Valid	T
DA1-Alt-Signal >= 2000_{THRES}	T

Macro

Dig2-Valid-and-Below

Description:

Comments:

References:

Appears in: Altitude2

DEFINITION

Dig2-alt = Valid	T
DA2-Alt-Signal < 2000_{THRES}	T

Macro

Dig2-Valid-and-Above

Description:

Comments:

References:

Appears in: Altitude2

DEFINITION

Dig-Alt2 = Valid	T
DA2-Alt-Signal >= 2000_{THRES}	T

Verification and Validation

Test Plan

Level 4
Design Representation

Environment

Physical Interfaces

Inputs

Analog Radio Altimeter Inputs

The representation of the radio altitude will be in the form of a single bit, i.e., bit 0 of Register 3. A zero in bit 0 will denote the altitude is above the threshold and a one in bit 0 will denote the aircraft is below the threshold.

The altitude status signal will be put into bit 1 of Register 3. A zero will indicate that the analog altitude value is invalid while a one will indicate the altitude signal is valid.

Digital Radio Altimeter Inputs

The digital altimeter word will be read from the bus and put into memory address ... The data will be stored in 17-bit 2'c complement form. The altitude will be in bits 29-13 with the sign in bit 29. The digital altitude status wil be in bits 31-30 with the following interpretation:

31	bf 30	**Values**	**Meaning**
0	0	FAIL	Failure Warning
0	1	NCD	No Computed Data
1	0	TEST	Functional Test
1	1	NORM	Normal Operation

DOI Status

A single bit where 0b means the DOI is not powered on while 1b means the DOI is powered on.

Inhibit

A single bit where 0b means do not inhibit the ASW while 1b means to inhibit the ASW.

Reset

The reset signal shall be received as a single bit with the value 0b denoting not to reset the ASW and 1b meaning that ASW should be reset.

Outputs

DOI Power

One bit with the meaning TBD

Watchdog Timer

The watchdog timer message shall consist of a single bit with 0b meaning do not strobe the watchdog timer and 1b denoting that the watchdog timer should be strobed.

Pilot–ASW Interface Design

Description of physical design, placement, etc.

Software Design Specification

Hardware Design Specification

Verification and Validation

Level 5
Physical Implementation

Aircraft Flight Manual Entries

Training

Physical Interface

The interface is implemented using an ARINC 429 bus. Characteristics of the ARINC-429 bus are defined in the ARINC-429 standard. Additional information specific to Digital Altimeters can be found in ARINC-707. This section contains the characteristics relevant to the ASW.

ARINC-429 words are 32 bits long. At low speed, each bit is presented in $83 \pm 2.5\% sec$. if using a 12 Mhz clock, $69 \pm 2.5\% sec$ if using a 14.5 Mhz clock with bit n+1 delivered before bit n. The first half of this period ($41.5 \pm 5\% sec$) is used to present the bit value as a signal high or low. The second half ($41.5 \pm 5\% sec$) is a null period during which the signal is null (neither high nor low). The interword gap is at least four bit times (333 sec).

Each bit is presented through two lines labeled line 1 and line 0. A 1b is presented as a signal high on line 1 and a signal low on line 0. A 0b is presented as a signal low on line 1 and high on line 0. A null signal on both lines indicates an absence of data (i.e., a null period or interword gap). A high or low signal on both lines should not occur.

Line 0	**Line 1**	*Meaning*
Null	Null	No Data
Hi	Low	0
Low	Hi	1

The format of ARINC-429 words with octal label is:

32	31..30	29	28..13	12	11	10..9	8..1
P	SM	S	DATA	PAD	FTI	SDI	LABEL

Relevant fields for the RTO include:

<table>
<tr><td>P</td><td>Bit 32 is set to ensure odd parity</td></tr>
<tr><td>SM</td><td>Bits 31-30 contain the Status Matrix (SM) and are interpreted as:
<table><tr><td>31</td><td>30</td><td>Meaning</td></tr><tr><td>0</td><td>0</td><td>Failure Warning</td></tr><tr><td>0</td><td>1</td><td>No Computed Data</td></tr><tr><td>1</td><td>0</td><td>Functional Test</td></tr><tr><td>1</td><td>1</td><td>Normal Operation</td></tr></table></td></tr>
<tr><td>S</td><td>Bit 29 contains the Sign (S) and is interpreted as 0 for a positive altitude and 1 for a negative altitude.</td></tr>
<tr><td>DATA</td><td>Bits 28-13 contain the altitude as encoded as 2's complement fraction of 8192 feet, where the decimal point is located to the left of bit 28. Note that a 1 in bit 16 thus represents an actual value of 1 and a 1 in bit 15 represents a value of 1/2.</td></tr>
<tr><td>LABEL</td><td>Bits 8-1 contain the octal label 164 (001 011 10b).</td></tr>
</table>

Inputs

Analog Radio Altimeter Inputs

The analog altimeter provides a real-valued estimate of the altitude as a voltage level.

The analog radio altitude shall be converted by the ASW hardware into a discrete signal on line AAA with high indicating that the aircraft is below the threshold altitude. The ASW hardware shall also generate a discrete signal on line AAV with high indicating if the analog altitude is valid.

[A wiring diagram would be helpful here.]

Digital Radio Altimeter Inputs

The 2_{DAnum} digital radio altitudes shall be received over 2_{DAnum} ARINC-429 low speed buses (see Appendix **??**). Bus 1 shall be on lines DA1-1 and DA1-2 and bus 2 shall be on lines DA2-1 and DA2-2. The ARINC words shall be assembled by the software as defined in ARINC-429. Only ARINC words with octal label 164 and correct parity shall be accepted.

If an acceptable altitude is not seen on the bus for more than a THRESH number of seconds, the bus shall be treated as inactive.

The digital altimeter reports altitude as a signed integer that represents a fraction of 8.192 feet.

DOI Status

The DOI status shall be received as a discrete signal on line STS with high indicating that the DOI is powered on.

Inhibit

The inhibit signal shall be received as a discrete signal on line 1HB with *high* indicating that the ASW should be inhibited.

Reset

The reset signal shall be received as a discrete signal on line RST with *high* indicating that the ASW should be reset to its initial state.

Outputs

DOI Power

The ASW shall turn power on to the DOI by setting the discrete signal on line PWR to high.

Watchdog Timer

(Unknown)

Software

Verification

TBD

Constants

Glossary

Index