**Plan for Hardware Aspects of Certification  
  
for the  
  
 ACMEY Company Avionics Passenger Counter**

Document No: 800-PHAC-01

Revision: 0.1

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | | \_\_\_\_\_\_\_\_\_\_\_ |
| Project Manager |  | Date | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_ | |
| Technical Project Lead |  | Date | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_ | |
| Principal Design Engineer |  | Date | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_ | |
| Principal Quality Engineer |  | Date | |

|  |
| --- |
| **Proprietary Notice**  This document and the information contained herein are the property of Airworthiness Certification Services LLC. Any reproduction, disclosure or use thereof is prohibited except as authorized in writing by Airworthiness Certification Services LLC. Recipient accepts the responsibility for maintaining the confidentiality of the contents of this document. |

|  |  |  |  |
| --- | --- | --- | --- |
| REVISIONS | | | |
| Rev. | Reason/Description | Requested/ Changed By | Date |
| 0.1 | Initial draft | N/A |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

**Section Page**

[1.0 INTRODUCTION 6](#_Toc228716421)

[1.1 Purpose 6](#_Toc228716422)

[1.2 Scope 6](#_Toc228716423)

[1.3 Part Number and Nomenclature 7](#_Toc228716424)

[1.4 Team Members 7](#_Toc228716425)

[1.5 Acronyms and Abbreviations 8](#_Toc228716426)

[1.6 Applicable Documents 9](#_Toc228716427)

[1.6.1 External Documents 9](#_Toc228716428)

[1.6.2 Internal Documents 9](#_Toc228716429)

[2.0 SYSTEM OVERVIEW 10](#_Toc228716430)

[2.1 System Functional Description 10](#_Toc228716431)

[2.2 System Architecture 10](#_Toc228716432)

[3.0 HARDWARE OVERVIEW 11](#_Toc228716433)

[3.1 Hardware Functions 11](#_Toc228716434)

[3.2 Hardware Architecture 11](#_Toc228716435)

[3.2.1 Computation 12](#_Toc228716436)

[3.2.2 Entry/Exit sensor 13](#_Toc228716437)

[3.2.3 Keypad Entry Panel 13](#_Toc228716438)

[3.2.4 Display Panel 13](#_Toc228716439)

[3.2.5 PIC Controller Interface & Fault Monitoring 14](#_Toc228716440)

[3.2.5.1 PIC Controller & ARINC 429 FPGA Interface 15](#_Toc228716441)

[3.3 Hardware Safety and Partitioning 16](#_Toc228716442)

[4.0 CERTIFICATION CONSIDERATIONS 17](#_Toc228716443)

[4.1 Certification Basis and Method of Compliance 17](#_Toc228716444)

[4.1.1 Hardware Design Assurance Levels 17](#_Toc228716445)

[4.1.2 Reference to TSO 18](#_Toc228716446)

[4.2 Hardware Level Determination 18](#_Toc228716447)

[5.0 HARDWARE DESIGN LIFECYCLE 19](#_Toc228716448)

[5.1 Hardware Planning Process 24](#_Toc228716449)

[5.1.1 Process Objectives and Activities 24](#_Toc228716450)

[5.1.2 Technical Interfaces 25](#_Toc228716451)

[5.1.3 Inputs 25](#_Toc228716452)

[5.1.4 Outputs 25](#_Toc228716453)

[5.1.5 Project Reviews 25](#_Toc228716454)

[5.1.6 Transition Criteria 26](#_Toc228716455)

[5.1.6.1 Transition Criteria for Entry into Planning Process 26](#_Toc228716456)

[5.1.6.2 Transition Criteria for Exit from Planning Process 27](#_Toc228716457)

[5.2 Requirements Capture Process 28](#_Toc228716458)

[5.2.1 Process Objectives and Activities 28](#_Toc228716459)

[5.2.2 Technical Interfaces 28](#_Toc228716460)

[5.2.3 Inputs 29](#_Toc228716461)

[5.2.4 Outputs 29](#_Toc228716462)

[5.2.5 Project Reviews 29](#_Toc228716463)

[5.2.6 Transition Criteria 30](#_Toc228716464)

[5.2.6.1 Transition Criteria For Entry Into Requirements Process 30](#_Toc228716465)

[5.2.6.2 Transition Criteria for Exit from Requirements Process 30](#_Toc228716466)

[5.3 Hardware Conceptual Design Process 32](#_Toc228716467)

[5.3.1 Process Objectives and Activities 32](#_Toc228716468)

[5.3.2 Technical Interfaces 32](#_Toc228716469)

[5.3.3 Inputs 32](#_Toc228716470)

[5.3.4 Outputs 32](#_Toc228716471)

[5.3.5 Project Reviews 33](#_Toc228716472)

[5.3.6 Transition Criteria 33](#_Toc228716473)

[5.3.6.1 Transition Criteria for Entry into Conceptual Design Process 33](#_Toc228716474)

[5.3.6.2 Transition Criteria for Exit from Conceptual Design Process 34](#_Toc228716475)

[5.4 Hardware Detailed Design Process 35](#_Toc228716476)

[5.4.1 Process Objectives and Activities 35](#_Toc228716477)

[5.4.2 Technical Interfaces 35](#_Toc228716478)

[5.4.3 Inputs 35](#_Toc228716479)

[5.4.4 Outputs 36](#_Toc228716480)

[5.4.5 Project Reviews 36](#_Toc228716481)

[5.4.6 Transition Criteria 37](#_Toc228716482)

[5.4.6.1 Transition Criteria For Entry Into Design Process 37](#_Toc228716483)

[5.4.6.2 Transition Criteria For Exit From Design Process 37](#_Toc228716484)

[5.5 Implementation Process 39](#_Toc228716485)

[5.5.1 Process Objectives and Activities 39](#_Toc228716486)

[5.5.2 Technical Interfaces 39](#_Toc228716487)

[5.5.3 Inputs 39](#_Toc228716488)

[5.5.4 Outputs 39](#_Toc228716489)

[5.5.5 Project Reviews 39](#_Toc228716490)

[5.5.6 Transition Criteria 40](#_Toc228716491)

[5.5.6.1 Transition Criteria for Entry into Implementation Process 40](#_Toc228716492)

[5.5.6.2 Transition Criteria for Exit from Implementation Process 40](#_Toc228716493)

[5.6 Hardware Production Transition Process 42](#_Toc228716494)

[5.6.1 Process Objectives and Activities 42](#_Toc228716495)

[5.6.2 Technical Interfaces 42](#_Toc228716496)

[5.6.3 Inputs 43](#_Toc228716497)

[5.6.4 Outputs 43](#_Toc228716498)

[5.6.5 Project Reviews 43](#_Toc228716499)

[5.6.6 Transition Criteria 44](#_Toc228716500)

[5.6.6.1 Transition Criteria for Entry into Production Transition Process 44](#_Toc228716501)

[5.6.6.2 Transition Criteria for Exit from Production Transition Process 44](#_Toc228716502)

[5.7 Hardware Validation and Verification Processes 46](#_Toc228716503)

[5.7.1 Process Objectives and Activities 46](#_Toc228716504)

[5.7.1.1 Elemental Analysis 48](#_Toc228716505)

[5.7.1.1.1 Elemental Analysis Method 48](#_Toc228716506)

[5.7.1.1.2 Elemental Analysis Results Resolution 48](#_Toc228716507)

[5.7.1.1.3 Elemental Analysis Lifecycle Data 49](#_Toc228716508)

[5.7.2 Technical Interfaces 49](#_Toc228716509)

[5.7.3 Transition Criteria 49](#_Toc228716510)

[5.8 Hardware Configuration Management Process 50](#_Toc228716511)

[5.8.1 Process Objectives and Activities 50](#_Toc228716512)

[5.8.2 Technical Interfaces 50](#_Toc228716513)

[5.8.3 Transition Criteria 50](#_Toc228716514)

[5.9 Process Assurance 51](#_Toc228716515)

[5.9.1 Process Objectives and Activities 51](#_Toc228716516)

[5.9.2 Technical Interfaces 52](#_Toc228716517)

[5.9.3 Transition Criteria 52](#_Toc228716518)

[5.9.4 Project Reviews 52](#_Toc228716519)

[5.10 Certification Liaison Process 53](#_Toc228716520)

[5.10.1 Process Objectives and Activities 53](#_Toc228716521)

[5.10.2 Technical Interfaces 53](#_Toc228716522)

[5.10.2.1 FAA Certification Consultant 54](#_Toc228716523)

[5.10.2.2 Systems and Equipment DER 56](#_Toc228716524)

[6.0 HARDWARE DESIGN LIFECYCLE DATA 57](#_Toc228716525)

[7.0 ADDITIONAL CONSIDERATIONS 60](#_Toc228716526)

[7.1 Use of Previously Developed Hardware 60](#_Toc228716527)

[7.1.1 ARINC 429 I/O FPGA 60](#_Toc228716528)

[7.1.1.1 Product Service Experience Data Acceptability Criteria 60](#_Toc228716529)

[7.1.1.1.1 Similarity – Application, Function, Operating Environment, and DAL 60](#_Toc228716530)

[7.1.1.1.2 Service Data Assessment 61](#_Toc228716531)

[7.2.1 ARINC 429 I/O FPGA Re-verification 62](#_Toc228716532)

[7.3 Use of Commercial-Off-The-Shelf (COTS) Components 62](#_Toc228716533)

[7.4 SH-1 Issue paper compliance 62](#_Toc228716534)

[7.4.1 Modifiable Devices 62](#_Toc228716535)

[7.4.2 Certification Plan 62](#_Toc228716536)

[7.4.3 Validation Processes 62](#_Toc228716537)

[7.4.4 Verification Processes 62](#_Toc228716538)

[7.4.5 Traceability 62](#_Toc228716539)

[7.4.6 Configuration Management 63](#_Toc228716540)

[7.4.7 Tool Assessment & Qualification 63](#_Toc228716541)

[7.4.8 Simple Electronic Hardware (SEH) 63](#_Toc228716542)

[7.4.9 Legacy Airborne Systems & Equipment Electronic Hardware 63](#_Toc228716543)

[7.4.10 Commercial Off-The-Shelf (COTS) Microprocessors 63](#_Toc228716544)

[7.4.11 Random Access Memory (RAM) based FPGAs 63](#_Toc228716545)

[7.5 Tool Assessment and Qualification 64](#_Toc228716546)

[7.5.1 Development Tools 64](#_Toc228716547)

[7.5.1.1 Qualification of Development Tools 65](#_Toc228716548)

[7.5.2 Verification Tools 66](#_Toc228716549)

[8.0 ALTERNATIVE METHODS 67](#_Toc228716550)

[9.0 CERTIFICATION SCHEDULE 68](#_Toc228716551)

[9.1 Project Schedule 69](#_Toc228716552)

[9.2 Certification Authority Web Interface 70](#_Toc228716553)

[9.3 Project-Level Integrated Compliance Management System 71](#_Toc228716554)

[9.3.1 SecureWeb Security Management System 72](#_Toc228716555)

[9.3.2 Problem Reporting Management System 73](#_Toc228716556)

[9.3.3 Document Review Management System 74](#_Toc228716557)

[9.3.4 Action Item Management System 75](#_Toc228716558)

[9.3.5 Requirements Traceability Management System 76](#_Toc228716559)

# INTRODUCTION

The ACMEY Passenger Counter System II S800-1000-01 is a new product based on the Legacy Passenger Counter System S800-1000-00. The Passenger Counter System II is updating the processor circuit card assembly with a new PIC microprocessor, Xlinix FPGA, and expanded functionality. The Legacy Passenger Counter II was a design assurance level (DAL) D product. The new Passenger Counter II will be developed to DAL B to accommodate future development for airline dispatch for total passenger count as a primary source which is a DAL B function.

## Purpose

The purpose of this *Plan for Hardware Aspects of Certification (PHAC)* is to describe how ACMEY co. will comply with the requirements and guidelines of DO-254 in the development and certification of the Passenger Counter IIproduct. Software aspects of certification are covered independently by ACMEY document, 800-PSAC-01, *Plan for Software Aspects of Certification, Passenger Counter System II.*

The PHAC, once approved, represents an agreement between the certification applicant and the certification authority on the processes and activities to be conducted and the resultant evidence to be produced to satisfy the hardware aspects of certification.

## Scope

It is the intent of this plan to describe the planning that will create the DO-254 compliant life cycle data needed to support the design approval of the Level B passenger counter FPGA. This plan also shows compliance to DO-254 for the Level C ARINC 429 FPGA using product’s service experience. Development of the Passenger Counter system will be preformed using the help of subcontractors in India.

This plan also includes the Hardware Design Plan (HDP), DO-254 section 10.1.2. The HDP describes the procedures, methods and standards to be applied and the processes and activities to be conducted for the design of the hardware item. It includes the Hardware Design Life Cycle, Hardware Product Description, Hardware Design Methods, Hardware Design Environment and Hardware Item Data.

The PHAC also covers the hardware description, the design life cycle of the hardware items, the hardware design assurance levels and the data items created during the design. This Plan for Hardware Aspects of Certification complies with the documentation requirements of RTCA/DO-254, Section 10.1.1 and 10.1.2.

## Part Number and Nomenclature

|  |  |
| --- | --- |
| **Part Number** | **Nomenclature** |
| S800-1000-01 | Avionics Passenger Counter |
| C800-1001-01 | Passenger Counter FPGA, 8 Bit Counter |
| C800-1010-00 | ARINC 429 I/o FPGA |

## Team Members

|  |  |
| --- | --- |
| **Name** | **Title** |
| John Smith | Project Manager |
| Tony Black | Systems Integration and Test |
| Debbie Brown | Reliability & Safety Engineer |
| Kenneth Johnson | Hardware Engineer |
| Ron Green | Hardware Configuration Management Engineer |
| Carol Sanders | Hardware Quality Assurance Engineer |
| Barbara Long | FAA Designated Engineering Representative |

## Acronyms and Abbreviations

AIMS Action Item Management System

ALU Arithmetic Logic Unit

ARP Aerospace Recommended Practice

ASIC Application Specific Integrated Circuit

DRMS Document Review Management System

HC1 Hardware Control Category 1

HC2 Hardware Control Category 2

COTS Commercial-Off-The-Shelf

EUROCAE European Organization for Civil Aviation Equipment

FAR Federal Aviation Regulations

FFP Functional Failure Path

FFPA Functional Failure Path Analysis

FHA Functional Hazard Assessment

F-FMEA Functional Failure Modes and Effects Analysis

FTA Fault Tree Analysis

HDL Hardware Description Language

JAR Joint Aviation Requirements

LRU Line Replaceable Unit

PHAC Plan for Hardware Aspects of Certification

PLD Programmable Logic Device

PSSA Preliminary System Safety Assessment

RTMS Requirements Traceability Management System

SAE Society of Automotive Engineers

SC Special Committee

SSA System Safety Assessment

WG Working Group

## Applicable Documents

The following documents are listed for reference only. Each document is applicable to this plan only to the extent specified herein.

### External Documents

RTCA/DO-254 Design Assurance for Airborne Electronic Hardware

FAA Order 8110.4C Type Certification

FAA Order 8110.105 FAA, Simple and Complex Electronic Hardware Approval Guidance

AC 20-152 Advisory Circular, RTCA Inc., Document DO-254, Design Assurance for Airborne Electronic Hardware

### Internal Documents

800-PHAC-01 Plan for Hardware Aspects of Certification (Ref. DO-254, 10.1.1)

800-PSAC-01 Plan for Software Aspects of Certification (Ref. DO-178B, 11.1)

800-HDP-01 Hardware Design Plan (Ref. DO-254, 10.1.2)

800-HVP-01 Hardware Verification Plan (Ref. DO-254, 10.1.4)

800-HCMP-01 Hardware Configuration Management Plan (Ref. DO-254, 10.1.5)

800-PAP-01 Hardware Process Assurance Plan (Ref. DO-254, 10.1.6)

800-HRD-01 Hardware Requirements Standards (Ref. DO-254, 10.2.1)

800-HDS-01 Hardware Design Standards (Ref. DO-254, 10.2.2)

800-HVVS-01 Validation and Verification Standards (Ref. DO-254, 10.2.3)

800-HRD-01 Hardware Requirements Document (Ref. DO-254, 10.3.1)

800-HDD-01 Hardware Design Data (Ref. DO-254, 10.3.2)

800-HTP-01 Hardware Test Procedures (Ref. DO-254, 10.4.4)

800-HLECI-01 Hardware Lifecycle Environment Configuration Index (Ref. CAST 27)

800-HCI-01 Hardware Configuration Index (Ref. CAST 27)

800-HAS-01 Hardware Accomplishment Summary (Ref. DO-254, 10.9)

# SYSTEM OVERVIEW

## System Functional Description

The Avionics Passenger Counter is a module that will keep track of how many passengers are currently in the aircraft/cabin. The current number of passengers in the cabin will be displayed on a display panel in real-time. The system will have a keypad entry so that the flight attendant can enter a passenger headcount correction/adjustment. The passenger headcount and any fault status information collected will be transmitted via ARINC 429 via the PIC processor and ARINC 429 I/O FPGA.

## System Architecture



The passenger headcount function is performed by counting the number of entries and exits. The module uses an Entry/Exit-Sensor to detect passengers’ movements in and out of the cabin. The number of passengers in the cabin is tracked by an up/down counter in an FPGA. The passenger load is displayed in real-time on the display panel. The keypad entry can asynchronously load the counter thereby adjusting/correcting the passenger load on the display/system.

# HARDWARE OVERVIEW

This section describes the hardware functions, hardware items, architecture, new technologies to be used, and any fail-safe, fault tolerant redundancy and partitioning techniques to be used.

## 3.1 Hardware Functions

There are five main hardware functions:

1. Computation (Derived)
2. Entry/Exit Detection
3. Keypad entry
4. Display
5. Fault monitoring and ARINC 429 data transmit

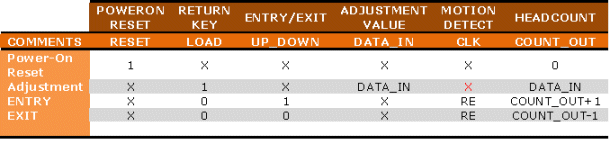
## 3.2 Hardware Architecture



### 3.2.1 Computation



The headcount function is done by an up/down counter inside the FPGA. Every time the Entry/Exit motion sensor detects an entry or an exit, the counter increments or decrements accordingly. Ever time the user presses return, the current headcount output is loaded with previously typed value. The truth table is shown below.



### 3.2.2 Entry/Exit sensor



The Entry/Exit Detection function is performed by the Entry/Exit sensor. This sensor will detect human motion and decipher whether the motion is inward or outward. The information is then sent to the FPGA for headcount computation.

### 3.2.3 Keypad Entry Panel



The headcount adjustment/correction data is generated by the keypad entry panel. This panel puts out a value typed by the user as well as a return key strobe signal. Both signals are sent to the FPGA for headcount adjustment/correction. The return key strobe signal is used to latch the value typed by the user into the FPGA logics.

### 3.2.4 Display Panel



The display panel simply displays the current headcount outputted by the FPGA.

### 3.2.5 PIC Controller Interface & Fault Monitoring



The Fault monitoring circuit monitors the sequences, timings and states of the Entry / Exit Detection sensor, Reset controller, keypad entry and the display panel. All of this information is fed to and analyzed by the PIC microcontroller. The PIC microcontroller’s software knows all the correct signal sequences, timing & states for all the interfaces. A fault is detected when a signal set is not within the predetermined constraints. The PIC controller then generates a fault message in the form able to fit into two 429 words which are sent to the FPGA. The FPGA then generates the appropriate serial ARINC 429 streams to the line driver which translates it out into the appropriate ARINC 429 signal level. The fault message is then sent to the maintenance computer via the ARINC 429 link. The cockpit multifunction display is used in maintenance aspects of the system. This is not a critical function and is used for maintenance and information only in the cockpit. The display reader provides the current passenger headcount to the flight attendant as the critical record for total headcount.

#### 3.2.5.1 PIC Controller & ARINC 429 FPGA Interface

The ARINC 429 FPGA is connected to the PIC Microcontroller via a standard 8-bit bus interface. There are 8-bit data, 8-bit address and a chip-select (CE) line. There is also one GPIO that is used as an iput to the PIC Microcontroller to indicate when the ARINC 429 FPGA is busy / sending data.



The ARINC 429 FPGA has to internal blocks: the Latch and the Shift Register. The Latch contains four 8-bit register that the Microcontroller can write to: each representing ¼ of the full ARINC 429 packet. These four register are made available to the next bloack in the form of a complete 32-bit bus/register to be loaded to the shift register. The Latch also contains a dummy register which, when written to, will send short pulse to the Shift Register. This short pulse will trigger the next block, the Shift register to load the data and serially shift out the data in the appropriate ARINC 429 forformat.

The final block in the ARINC 429 FPGA is the Shift Register. This block is really combination of a state machine and a shift register (shown in the figure below). The sole purpose of this block is to serially shift the 32-bit ARINC 429 data with the appropriate timings.



When a fult is detected, the PIC controller determines that a message needs to be sent. It internally contruct the 32-bit ARINC 429 packet in four bytes and writes them out into the FPGA Registers. The Microcontroller then waits for the Busy signal (from the FPGA Shift Register block) to indicate a ready state (inactive). When the Busy signal indicates a “ready” state, the the controller writes to a dummy register to initiate the serial transfer.

## 3.3 Hardware Safety and Partitioning

The system is composed of diagnostics and other fail-safe mechanisms used to ensure that failures of the system are detected and that the system goes to a safe state if it's unable to perform a safety function. The hardware will be designed so that it will continue to operate, possibly at a reduced level, rather than failing completely, when some part of the system fails. During this condition, a visible fault indication will be present.

# CERTIFICATION CONSIDERATIONS

## Certification Basis and Method of Compliance

The certification basis for the software is RTCA/DO-254. This certification will be accomplished as part of the lifecycle development. The Quality Assurance Engineer will compile applicable artifacts and submit them to the Certification Authority. Verification objectives are satisfied through a combination of reviews and analysis, the development of test cases and procedures, and the subsequent execution of those test procedures. Reviews and analysis provide an assessment of the accuracy, completeness, and verifiability of the requirements, architecture, and design implementation.

The System Safety Assessment revealed that failure conditions which would prevent continued safe flight and landing. The applicable Failure Condition Category is **Catastrophic**. Hardware whose anomalous behavior would cause or contribute to a failure of system function resulting in a catastrophic failure condition for the aircraft is identified as **Level A**. Due to the FAA part 23 specific policy memo, the passenger counter will be developed to level B.

|  |  |  |  |
| --- | --- | --- | --- |
| **Function** | **System Failure** | **Criticality** | **Required Hardware Certification Level Per AC 2x.1309-1C** |
| Function 01 | Failure 01 | Hazardous | B |
| Function 02 | Failure 02 | Minor | D |
| Function 03 | Failure 03 | Hazardous | B |
| Passenger count | Incorrect count | Catastrophic | A |
| Function 05 | Failure 05 | Hazardous | B |
| Function 06 | Failure 06 | Major | C |
| Function 07 | Failure 07 | Major | C |
| Function 08 | Failure 08 | Hazardous | B |

The SSA determines the passenger count to be a catastrophic failure due to the airline needs for dispatch. The aircraft is a part 23 aircraft and will reduce this to level B based on FAA policy memo; *Applying Advisory Circular 20-152, “RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware,” to Title 14 Code of Federal Regulations, Part 23 Aircraft; PS-ACE100-2005-50001.*

### Hardware Design Assurance Levels

|  |  |  |  |
| --- | --- | --- | --- |
| **Hardware Unit** | **hardware Name** | **Design Assurance Level** | **Justification for Design Assurance Level** |
| 8 Bit Counter | FPGA | B | See Section 4.1.1 |
| ARINC 429 I/O | FPGA | C | See Section 4.1.1 |

### Reference to TSO

The product was developed in compliance with the following TSO:

|  |  |
| --- | --- |
| Reference / Issue | Description |
| FAA TSO-C246 | TSO, Avionics Passenger Counter |
| FAA Order 8110.4C | Type Certification |

## Hardware Level Determination

Hardware Level determination was based on the Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA) and System Safety Assessment (SSA).

| **DO-254 Objectives By Design Assurance Level** | | | |
| --- | --- | --- | --- |
| **Level** | **Failure Condition** | **DO-254 Objectives** | **Objectives Satisfied With Independence** |
| **A** | Catastrophic | 39 | Process Assurance and Verification Objectives |
| **B** | Hazardous | 39 | Process Assurance and Verification Objectives |
| **C** | Major | 37 | Process Assurance Objectives |
| **D** | Minor | 31 | Process Assurance Objectives |
| **E** | No Effect | NA | NA |

# HARDWARE DESIGN LIFECYCLE

This section describes the procedures, methods and standards to be applied and processes and activities to be performed to meet the hardware design assurance objectives. It describes the activities, combinations and sequencing of activities, relationships between processes and activities, transition criteria, responsibilities, tool usage, and means for providing feedback and interaction among hardware processes and between hardware processes and the system and software processes. This section may reference applicable plans, policies, standards, procedures and deviations to those plans and standards for the program.

The hardware Lifecycle includes the following processes:

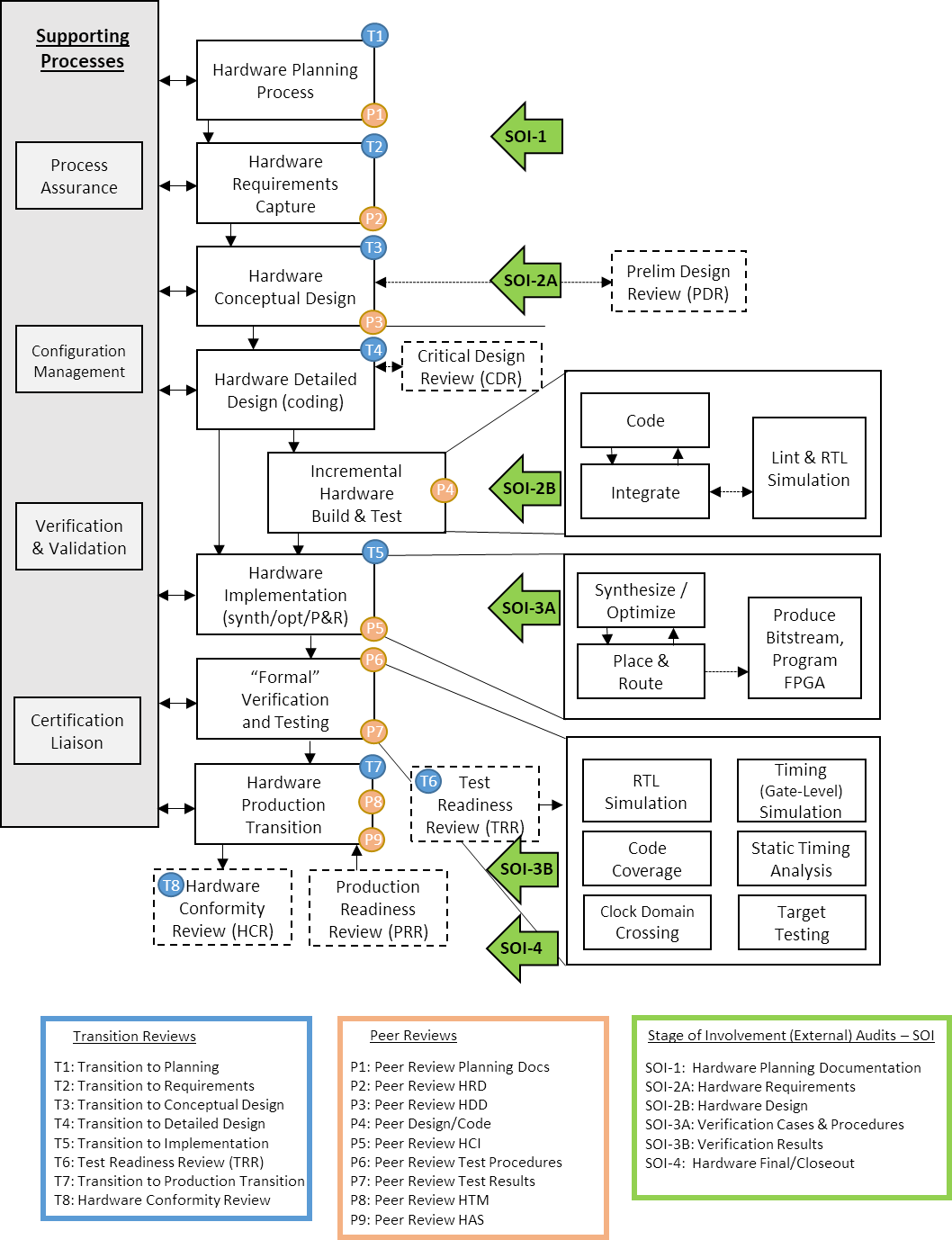
* Hardware Planning Process (See Section 5.1).
* Hardware Development Process
  + Requirements Capture Process (See Section 5.2).
  + Hardware Conceptual Design Process (See Section 5.3).
  + Hardware Detail Design Process (See Section 5.4).
  + Hardware Implementation Process (See Section 5.5).
  + Hardware Product Transition Process (See Section 5.6).

Integrated into and integral to each of these processes is the:

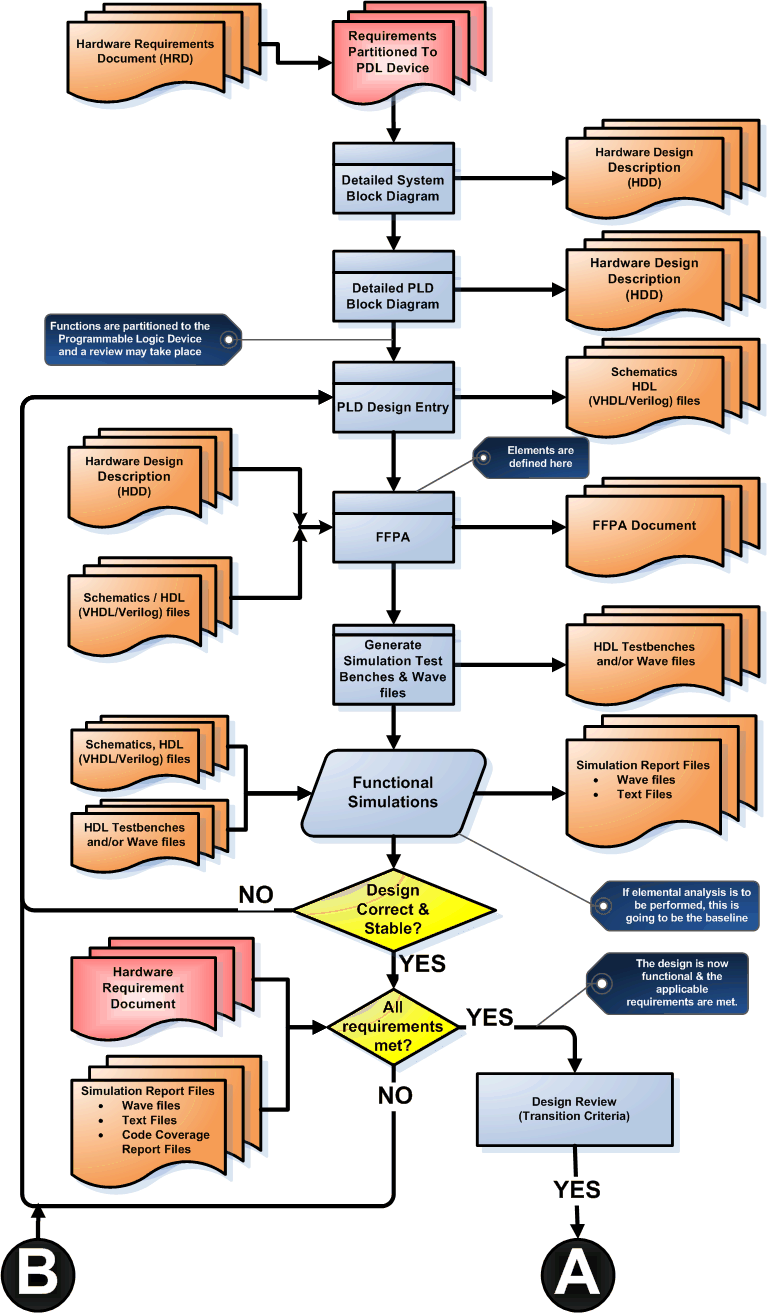
* Hardware Validation and Verification Process (See Section 5.7).
* Hardware Configuration Management Process (See Section 5.8).
* Hardware Process Assurance (See Section 5.9).
* Certification Liaison Process (See Section 5.10).

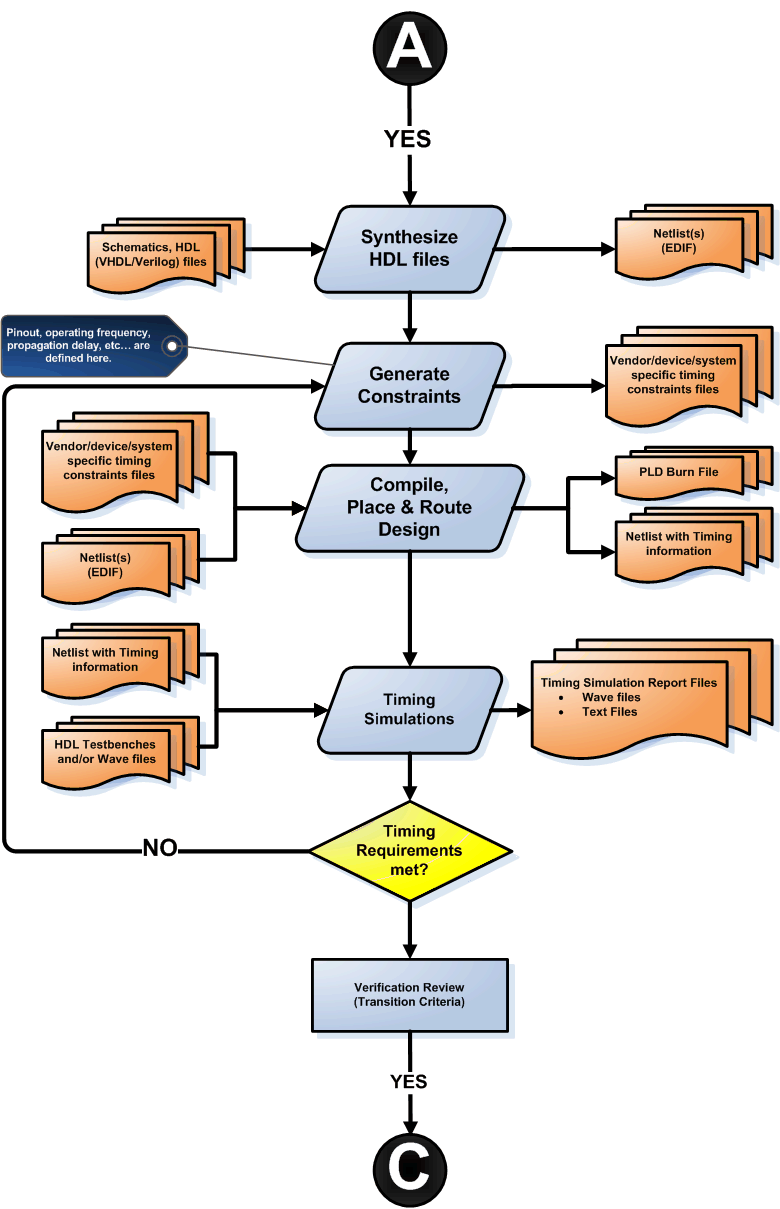
Elements of each process are defined in a Web interface. Details of the activities document description and transition criteria are further described in the following paragraphs. Specific process implementation is described in the Program Plans.

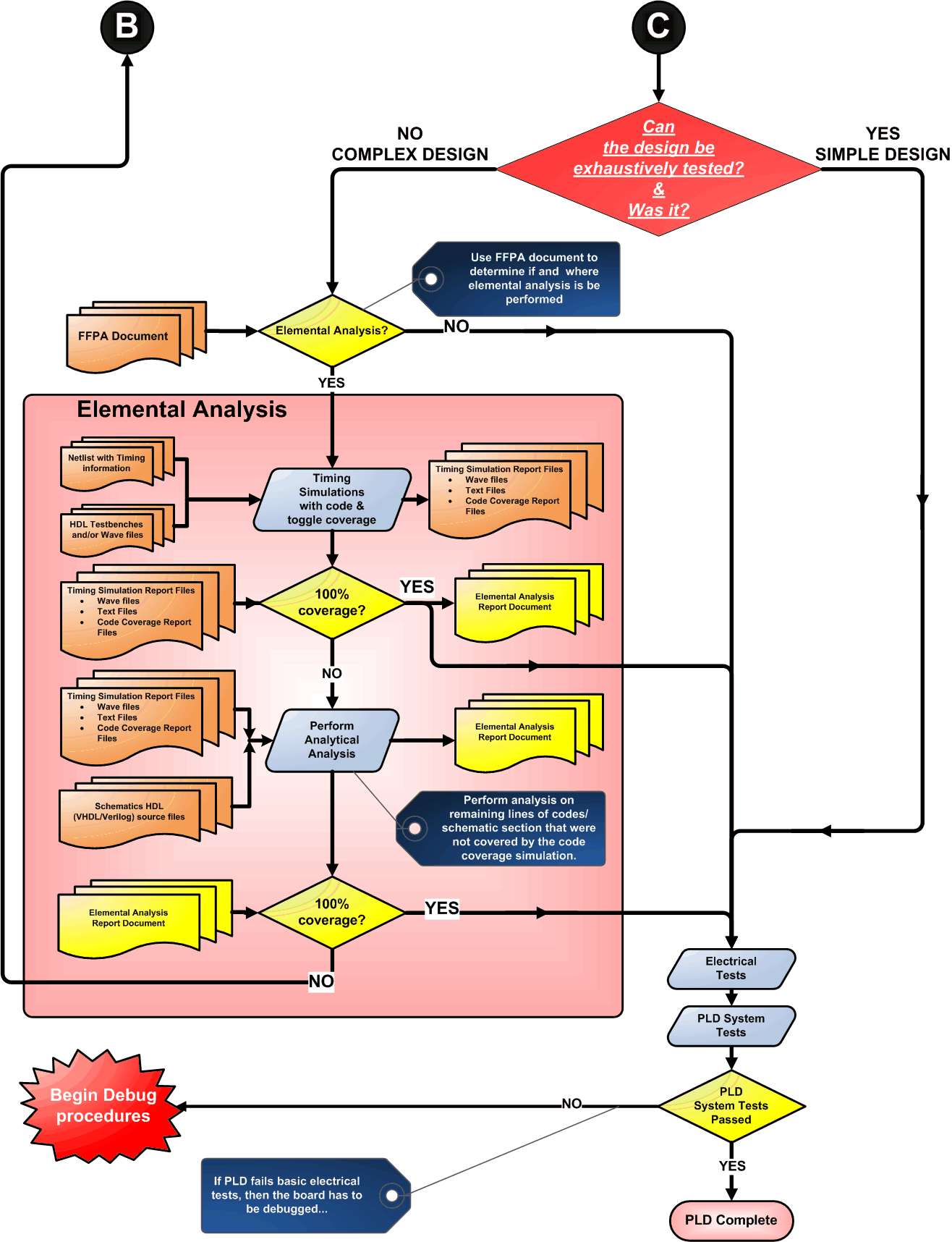
The following Lifecycle Flow Diagram summarizes the planned project waterfall lifecycle approach in terms of inputs, processes, and outputs.



The following Design Flow details the planned complex electronic hardware design-specific lifecycle in terms of inputs, processes, and outputs. It also identifies the key transition points.







## Hardware Planning Process

The purpose of the hardware planning process is to define the means by which the functional and airworthiness requirements are converted into a hardware item with an acceptable amount of evidence of assurance that the item will safely perform its intended functions.

The following planning documents and checklists will be reviewed:

* Plan for Hardware Aspects of Certification
* Hardware Design Plan
* Hardware Verification Plan
* Hardware Configuration Management Plan
* Hardware Process Assurance Plan
* Hardware Requirements Standards
* Hardware Design Standards
* Validation and Verification Standards
* Hardware Archive Standards
* Review Checklists (See Action Item Management System in Hardware QA Plan)
* Document Checklists (See Document Review Management System in Hardware QA Plan)

### Process Objectives and Activities

Objectives of the Planning Process:

* The hardware design life cycle processes are defined.
* Standards are selected and defined.
* The hardware development and verification environments are selected or defined.
* The means of compliance of the hardware design assurance objectives, including strategies, are proposed to the certification authority.

Activities of the Planning Process:

* The hardware design life cycle processes, including transition criteria, if applicable, and the inter-relationships between the individual processes, such as their sequencing and feedback mechanisms, are defined.
* The proposed design methods are defined and explained. This includes consideration of the expected hardware design and the rationale of the proposed verification methods.
* Hardware design standards, if any are to be used for the project, including acceptable deviations from the standards, are identified. These may range from generic quality standards to company or program specific standards.
* The means of achieving coordination between the hardware design processes and the supporting processes, with particular attention to activities associated with systems, complex hardware and aircraft certification, are determined.
* The activities of each hardware design process and associated supporting processes are defined. The definitions are at a level that enables the hardware design process and associated supporting processes to be controlled.
* The design environment is chosen, including the tools, procedures and hardware that are to be used to develop, verify and control the hardware item and the life cycle data.
* If certification credit is sought for use of tools in combination, the sequence of operation of the tools is specified in the respective plan.
* The process for deviating from the established plans, if deviations become necessary and affect certification, are identified.
* The policies, procedures, standards and methods to be used to identify, manage, and control the hardware, the associated baselines, and the hardware design life cycle data are described.
* The policies and procedures for implementation of process assurance of the hardware design processes are described.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware Process Assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Hardware Planning Process.

### Inputs

The System Safety Assessment, certification considerations, industry, regulatory and system requirements are inputs to the Hardware Planning Process. In addition, engineering feasibility, resource analysis, cost and schedule are also inputs to the Hardware Planning Process.

### Outputs

The following documents are produced or updated by the Hardware Planning Process: Plan for Hardware Aspects of Certification; Hardware Configuration Management Plan; Hardware process assurance Plan; Hardware Development Plan; Hardware Verification Plan.

### Project Reviews

Attendance at the project reviews is mandatory for Hardware Engineering, Hardware Engineering, Mechanical Engineering, Quality Assurance and Program Management. Other disciplines such as Marketing, Product Support and Senior Management may participate in the reviews if required. In addition, the customer may be invited to reviews.

Hardware Planning Review

The Hardware Planning Process concludes with a Hardware Planning Review conducted by the Project Engineer. Transition Criteria from the Hardware Planning Process to the Hardware Development Process are discussed at this review.

When the Hardware Planning Review is held, action items are recorded in the Action Item Management System database file associated with that review. The review includes a discussion of the status of the development and integral activities, a review and status of the Planning Documents, and a discussion of any special considerations. The Hardware process assurance representative steps through the Hardware Planning Review Checklist. If deficiencies are revealed during the review, action items are generated, and corrective actions to resolve the deficiencies are fed back into the appropriate process.

Lifecycle data to be considered at the Hardware Planning Review include the following:

* Review and approval of the Plan for Hardware Aspects of Certification
* Review and approval of the Hardware Design Plan
* Review and approval of the Hardware Verification Plan
* Review and approval of the Hardware Configuration Management Plan
* Review and approval of the Hardware Process Assurance Plan
* Review and approval of the Hardware Requirements Standards
* Review and approval of the Hardware Design Standards
* Review and approval of the Validation and Verification Standards
* Review and approval of the Hardware Archive Standards

### Transition Criteria

#### Transition Criteria for Entry into Planning Process

Objective evidence of Pre-Planning Process activities are completed and verified. Pre-Planning Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* Project cost and schedule have been approved and resources allocated
* Definition and feasibility of Industry Requirements
* Definition and feasibility of Regulatory Requirements
* Definition and feasibility of System Requirements
* Definition and feasibility of Customer Requirements

#### Transition Criteria for Exit from Planning Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Planning Process activities are complete and verified. Planning Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* Plan for Hardware Aspects of Certification
* Hardware Design Plan
* Hardware Verification Plan
* Hardware Configuration Management Plan
* Hardware Process Assurance Plan
* Hardware Requirements Standards
* Hardware Design Standards
* Validation and Verification Standards
* Hardware Archive Standards
* Review Checklists (See Action Item Management System in Hardware QA Plan)
* Document Checklists (See Document Review Management System in Hardware QA Plan)

The following additional transition criteria are required:

* Coordination between Hardware Development and Integral Processes is established
* Means to revise Hardware Plans were established
* Hardware Plans and standards are placed under change control and reviews are complete
* Deactivated code, user-modifiable code and field-loadable code handling are addressed

## Requirements Capture Process

The requirements capture process identifies and records the hardware item requirements. This includes those derived requirements imposed by the proposed hardware item architecture, choice of technology, the basic and optional functionality, environmental, and performance requirements as well as the requirements imposed by the system safety assessment. This process may be iterative since additional requirements may become known during design.

### Process Objectives and Activities

The Requirements Process establishes the capabilities of the hardware and the conditions for the hardware design.

Objectives of the Requirements Process:

* Requirements are identified, defined, and documented. This includes allocated requirements from the PSSA and derived requirements from the hardware safety assessment.
* Derived requirements produced are fed back to the appropriate process.
* Requirement omissions and errors are provided to the appropriate process for resolution.

Activities of the Requirements Process:

* The system requirements allocated to the hardware item are documented. These may include identifying requirements, such as functionality and performance, and architectural considerations, such as segregation, Built-In-Test, testability, external interfaces, environment, test and maintenance considerations, power, and physical characteristics.
* The safety requirements from the PSSA related to the hardware item are identified.
* Design constraints due to production processes, standards, procedures, technology, design environment, and design guidance are identified.
* Derived requirements necessary for implementation are determined. Requirements derived from the hardware safety assessment that have safety implications are uniquely identified.
* Derived requirements are fed back to the SSA process so that the effects on the system requirements can be assessed.
* The requirement data is documented in quantitative terms, with tolerances where applicable. This does not include the description of design or verification solutions.
* Requirement omissions or errors discovered during this process are provided to the system development process.
* The requirements, including those generated to meet the PSSA requirements, are traceable to the next higher hierarchical level of requirements. Derived requirements are identified and traced as far as possible through the hierarchical levels.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware Process Assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Requirements Capture Process. In addition, Engineering meets with Representatives from Marketing, Sales, Manufacturing Test Engineering, and Quality Assurance to discuss the Hardware Requirements.

### Inputs

Marketing Requirements and Regulatory Specifications, such as ARINC, RTCA, and other documents, are used as inputs to the Hardware Requirements Analysis Process. The Hardware Requirements Standards are used as inputs to define the methods, rules and tools to be used to develop the high-level requirements.

### Outputs

The Hardware Requirements Document will be produced or updated as a result of the Hardware Requirements Definition Process.

### Project Reviews

Hardware Requirements Review

The Hardware Requirements Review follows the Hardware Requirements Definition Process. The Project Engineer conducts the Hardware Requirements Review using the Hardware Review Checklist as an aid. When the Hardware Requirements Review is held, the Project Engineer records the minutes or assign someone to do so. The minutes include a discussion of the results, agreements and disagreements reached during the review, updates to the project schedule, resource estimates, and action item assignments with estimated completion dates.

The review is conducted to achieve the project team’s consensus of the correctness of the hardware requirements. Members of the project team, which includes the Project Engineer, Hardware Engineer assigned to the project, Hardware Engineer, Hardware process assurance Engineer, and the Configuration Management representative, will be present at the review. Other concerned individuals, such as Manufacturing Test Engineering, Marketing or Sales, may be invited. The review will include a presentation of the naming conventions used for the hardware requirements and a review and discussion of each hardware requirement.

The objective of the Hardware Requirements Review is to detect and report errors that may have been introduced during the Hardware Requirements Definition Process.

* The review ensures that the system functions to be performed by the hardware are completely defined, that the performance and safety requirements have been correctly reflected in the hardware requirements, and that justification is provided for any derived requirements.
* The review ensures that each requirement is accurate, unambiguous and sufficiently detailed, and that the requirements do not conflict with each other.
* The review confirms that no conflicts exist between the high-level requirements and the hardware features of the target system. Special attention is given to the use of system resources, system response times and input/output hardware.
* The review ensures that each requirement can be verified.

The Hardware Quality Engineer steps through the Hardware Review Checklist. If deficiencies are revealed during the review, action items are generated, and corrective actions to resolve the deficiencies are fed back into the appropriate process.

Items to be considered at the Hardware Requirements Review include, but are not limited to, the following:

* Review and approval of the Hardware Requirements Document.
* Review and acceptance of all functional requirements, performance requirements, interface requirements and design constraints.
* High-level and Derived requirements are recorded in the Hardware Requirements Document.
* The top-level hardware design is documented in the preliminary release of the Hardware Design Description.
* The Requirements Capture Process includes a Hardware Preliminary Design Review. Following the review, the program proceeds to the Hardware Design process.

### Transition Criteria

#### Transition Criteria For Entry Into Requirements Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Planning Process activities are complete and verified. Planning Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* Plan for Hardware Aspects of Certification
* Hardware Design Plan
* Hardware Verification Plan
* Hardware Configuration Management Plan
* Hardware Process Assurance Plan
* Hardware Requirements Standards
* Hardware Design Standards
* Validation and Verification Standards
* Hardware Archive Standards

The following additional transition criteria are required:

* Coordination between Hardware Development and Integral Processes was established.
* Means to revise Hardware Plans were established.
* Hardware Plans and standards are placed under change control and reviews are completed.
* Deactivated code, user-modifiable code, and field-loadable code handling are addressed.

#### Transition Criteria for Exit from Requirements Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Requirements Process activities are complete and verified. Requirements Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* High-Level Hardware Requirements Traceable To System Requirements
* System Requirements Document
* Hardware Requirements Document

The following additional transition criteria are required:

* The system and interface requirements allocated to hardware are analyzed for ambiguities, inconsistencies, and undefined conditions.
* Each system requirement that was allocated to hardware was specified in the high-level requirements.
* High-level hardware requirements that affect system hazards are defined.
* The high-level requirements conformed to the Hardware Requirements Standards.
* The high-level requirements are verifiable and consistent.
* The high-level requirements are stated in quantitative terms with tolerances where applicable.
* Each system level requirement allocated to hardware was traceable to one or more system requirements.
* Each high-level requirement was traceable to one or more system requirements, with the exception of derived requirements.
* Errors/deficiencies discovered during the Requirements Capture Process are fed back into the system life cycle process for clarification and/or correction.

## Hardware Conceptual Design Process

The conceptual design process produces a high-level design concept that may be assessed to determine the potential for the resulting design implementation to meet the requirements. This may be accomplished using such items as functional block diagrams, design and architecture descriptions, circuit card assembly outlines, and chassis sketches.

### Process Objectives and Activities

Objectives of the Conceptual Design Process:

* The hardware item conceptual design is developed consistent with its requirements.
* Derived requirements produced are fed back to the requirements capture or other appropriate processes.
* Requirement omissions and errors are provided to the appropriate processes for resolution.

Activities of the Conceptual Design Process:

* A high-level description is generated for the hardware item. This may include architectural constraints related to safety, including those necessary to address design errors and functional, component over-stress, reliability and robustness defects and identification of any implementation constraints on complex hardware or other system components.
* Major components are identified. The way they contribute to the hardware safety requirements are determined, including the impact of unused functions.
* Derived requirements, including the interface definition, are fed back to the requirements capture process.
* Requirement omissions and errors are fed back to the appropriate process for resolution.
* The reliability, maintenance and test features to be provided are identified.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware process assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Hardware Design Process.

### Inputs

The Marketing Requirements, Hardware Requirements Document and Regulatory Specifications, such as ARINC, RTCA, and other documents, are used as inputs to the Hardware Design Process. Hardware Block diagrams, Flow diagrams, and State Transition Diagrams prepared during the Requirements Process, are updated and used as input to the Hardware Design Process. The Hardware Design Standards are used as inputs to define the methods, rules and tools to be used to develop the hardware architecture and design.

### Outputs

Outputs from the Hardware Design Process include the Hardware Design Description, control flow diagrams, data flow diagrams, state transition diagrams, or Flow Charts (as applicable). An additional output of this process includes the Allocated Baseline established by the Configuration Management Representative.

### Project Reviews

Hardware Preliminary Design Review

The Hardware Preliminary Design Review (PDR) follows the Hardware Requirements Review. The Hardware PDR Checklist is used during the review.

Representatives from Electrical, Mechanical, Hardware, Quality Assurance, Manufacturing Engineering, and Manufacturing Test Engineering are invited to the Hardware PDR.

The Project Engineer conducts the Hardware PDR. The review includes a presentation of the overall hardware design structure, module design structure, relationships of the design elements and modules, and rationale for the hardware design.

The interfaces between the hardware modules and interfaces between the hardware and hardware devices are presented and discussed.

If deficiencies are revealed during the review, action items are generated, and corrective actions to resolve the deficiencies are fed back into the appropriate process.

Where applicable, the following items considered at the PDR include:

* Hardware Architecture
* Rationale for the Hardware Design
* Review and approval of the Context Level Data Flow Diagram
* Review and approval of the Hardware Block Diagrams
* Review and approval of Control Flows and Data Flows
* Review and approval of State Transition Diagrams

### Transition Criteria

#### Transition Criteria for Entry into Conceptual Design Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Requirements Process activities are complete and verified. Requirements Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* High-Level Hardware Requirements Traceable To System Requirements
* System Requirements Document
* Hardware Requirements Document

The following additional transition criteria are required:

* The system and interface requirements allocated to hardware are analyzed for ambiguities, inconsistencies, and undefined conditions.
* Each system requirement that was allocated to hardware was specified in the high-level requirements.
* High-level hardware requirements that affect system hazards are defined.
* The high-level requirements conformed to the Hardware Requirements Standards.
* The high-level requirements are verifiable and consistent.
* The high-level requirements are stated in quantitative terms with tolerances where applicable.
* Each system level requirement allocated to hardware was traceable to one or more system requirements.
* Each high-level requirement was traceable to one or more system requirements, with the exception of derived requirements.
* Requirements errors or deficiencies discovered are fed back into the system life cycle process for clarification and/or correction.

#### Transition Criteria for Exit from Conceptual Design Process

Objective evidence (e.g., Meeting minutes, Action Items, and Document Review Checklists) of Design Process activities are complete and verified. Design Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* Hardware Design Traceable To High-Level Requirements
* Hardware Design Description

The following additional transition criteria are required:

* The hardware architecture developed during the Hardware Conceptual Design Process conforms to the Hardware Design Standards.
* The hardware architecture is traceable to the high-level requirements.
* The hardware design is verifiable and consistent.
* Derived requirements are identified.
* Derived requirements are analyzed to ensure that the high-level requirements are not compromised.
* The control flows and data flows are verified.
* Failure condition response is determined consistent with safety-related requirements.
* Errors/deficiencies discovered during the Hardware Design Process are fed back into the system life cycle process for clarification and/or correction.

## Hardware Detailed Design Process

The conceptual design process produces a high-level design concept that may be assessed to determine the potential for the resulting design implementation to meet the requirements. This may be accomplished using such items as functional block diagrams, design and architecture descriptions, circuit card assembly outlines, and chassis sketches. The detailed design process produces detailed design data using the hardware item requirements and conceptual design data as the basis for the detailed design.

### Process Objectives and Activities

Objectives of the Detailed Design Process:

* The detailed design is developed from the hardware item requirements and conceptual design data.
* Derived requirements are fed back to the conceptual design process or other appropriate processes.
* Requirement omissions or errors are provided to the appropriate processes for resolution.

Activities of the Detailed Design Process:

* The detailed design data for the hardware item are generated based on the requirements and conceptual design data. This may include assembly and interconnection data, component data, HDL, test methods and hardware-software interface data.
* Architectural design techniques are implemented as necessary. These may include establishing safety monitors for proper functionality, dissimilarity between function and safety monitors, preclusion of a design error from impacting safety, and fault tolerant designs.
* Test features are designed in, where necessary, to allow verification of safety requirements.
* An assessment of unused functions is performed to identify potential effects on safety. Adverse effects are addressed.
* Constraints on the design, installation or operation of the hardware item that, if not adhered to, could affect the safety of the item are identified.
* Derived requirements produced during the detailed design process are fed back to the conceptual design or other appropriate processes.
* Requirement omissions and errors discovered during the detailed design process are provided to the appropriate process for resolution.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware process assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Hardware Design Process.

### Inputs

The Marketing Requirements, Hardware Requirements Document and Regulatory Specifications, such as ARINC, RTCA, and other documents, are used as inputs to the Hardware Design Process. Hardware Block diagrams, Flow diagrams, and State Transition Diagrams prepared during the Requirements Process, are updated and used as input to the Hardware Design Process. The Hardware Design Standards are used as inputs to define the methods, rules, and tools to be used to develop the hardware architecture and design.

### Outputs

Outputs from the Hardware Detailed Design Process include the Hardware Design Description, control flow diagrams, data flow diagrams, state transition diagrams, or Flow Charts (as applicable). An additional output of this process includes the Allocated Baseline established by the Configuration Management Representative.

### Project Reviews

Hardware Critical Design Review

The Hardware Critical Design Review (CDR) is integrated into the Hardware Detailed Design process. The Hardware CDR Checklist will be used during the review.

The Project Engineer conducts the Hardware CDR. Representatives from Electrical, Hardware, Mechanical, Marketing, Quality Assurance, Manufacturing, and Test Departments may be invited to attend the Hardware CDR.

The review includes a presentation by the hardware engineer of the overall detailed design structure, module design structure, relationships of the design elements and modules, and rationale for the hardware design.

The interfaces between the hardware modules and interfaces between the hardware and hardware devices will be presented and discussed.

The Hardware CDR ensures that the components of the hardware architecture are accurate and consistent. The review will confirm that no conflicts exist between the hardware architecture and the hardware features of the target system.

If deficiencies are revealed during the review, corrective actions to resolve the deficiencies are fed back into the appropriate engineering process or document. This may include the Marketing Requirements, Hardware Requirements Document, the Electrical Design, Mechanical Design, or the Hardware Design.

One or more of the following items will be considered at the Hardware CDR:

* Hardware requirements are complete
* The Hardware Detailed Design conforms to the requirements
* Review and approval of the Context Level Data Flow Diagram
* Review and approval of the Hardware Block Diagram
* Review and approval of Control Flow and Data Flow

When the Hardware CDR is held, the Project Engineer records Action Items or assigns someone to do so. The Action Items include action item assignments.

### Transition Criteria

#### Transition Criteria For Entry Into Design Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Requirements Process activities are completed and verified. Requirements Process artifacts are produced, base-lined, reviewed, and under configuration management control including:

* High-Level Hardware Requirements Traceable To System Requirements
* System Requirements Document
* Hardware Requirements Document

The following additional transition criteria are required:

* The system and interface requirements allocated to hardware are analyzed for ambiguities, inconsistencies, and undefined conditions.
* Each system requirement that was allocated to hardware was specified in the high-level requirements.
* High-level hardware requirements that affect system hazards are defined.
* The high-level requirements conformed to the Hardware Requirements Standards.
* The high-level requirements are verifiable and consistent.
* The high-level requirements are stated in quantitative terms with tolerances where applicable.
* Each system level requirement allocated to hardware was traceable to one or more system requirements.
* Each high-level requirement was traceable to one or more system requirements, with the exception of derived requirements.
* Errors/deficiencies discovered during the Requirements Capture Process are fed back into the system life cycle process for clarification and/or correction.

#### Transition Criteria For Exit From Design Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Design Process activities are complete and verified. Design Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* Hardware Design Traceable To High-Level Requirements
* Hardware Design Description

The following additional transition criteria are required:

* The hardware architecture developed during the Hardware Design Process conformed to the Hardware Design Standards.
* The hardware architecture are traceable to the high-level requirements.
* The hardware design is verifiable and consistent.
* The derived requirements are defined.
* The derived requirements are analyzed to ensure that the high-level requirements are not compromised. The control flows and data flows are verified.
* Failure condition response was determined consistent with safety-related requirements.
* Errors/deficiencies discovered during the Hardware Design Process are fed back into the system life cycle process for clarification and/or correction.

## Implementation Process

The implementation process uses the detailed design data to produce the hardware item that is an input to the testing activity.

### Process Objectives and Activities

Objectives of the Implementation Process:

* A hardware item is produced which implements the hardware detailed design using representative manufacturing processes.
* The hardware item implementation, assembly and installation data is complete.
* Derived requirements are fed back to the detailed design process or other appropriate processes.
* Requirement omissions and errors are provided to the appropriate processes for resolution.

Activities of the Implementation Process:

* A hardware item is produced using the design data and, where practical, the resources intended for the production product. This may include procurement, kiting, build, inspection and test.
* Derived requirements generated by the implementation process are fed back to the detailed design process or other appropriate processes.
* Omissions and errors discovered during the implementation process are provided to the appropriate process for resolution.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware process assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Implementation Process.

### Inputs

The Hardware Design Standard along with project specific design documents are inputs to the Implementation process. The Hardware Code Standards are used as inputs to define the programming language(s), methods, rules and tools to be used to code.

### Outputs

Hardware files can be used to generate hardware listings if needed. Other outputs include complexity and other Quality metrics.

### Project Reviews

Hardware Implementation Review

The Hardware Implementation Review is integrated into the Hardware Implementation process. The Hardware Implementation Review Checklist will be used during the review.

The Project Engineer conducts the Hardware Implementation Review. Representatives from the Electrical, Hardware, Quality Assurance, Manufacturing, and Test Departments may be invited to attend the Hardware Implementation Review.

The review consists of evaluations of the hardware implementation in its source language against the Hardware Design Data for compliance and completeness.

If deficiencies are revealed during the review, corrective actions to resolve the deficiencies are fed back into the appropriate engineering process or document. This may include the Marketing Requirements, Hardware Requirements Document, the Electrical Design, Mechanical Design, or the Hardware Design.

One or more of the following items will be considered at the Hardware Implementation Review:

* Hardware design is complete
* The Hardware Implementation complies with the Hardware Design
* The Hardware Implementation is complete with respect to the Hardware Design

When the Hardware Implementation Review is held, the Project Engineer records Action Items or assigns someone to do so. The Action Items include action item assignments.

### Transition Criteria

#### Transition Criteria for Entry into Implementation Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Design Process activities are complete and verified. Design Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* Hardware Design Traceable To High-Level Requirements
* Hardware Design Description

The following additional transition criteria are required:

* The hardware architecture developed during the Hardware Design Process conforms to the Hardware Design Standards.
* The hardware architecture is traceable to the high-level requirements.
* The hardware design is verifiable and consistent.
* Derived requirements are identified.
* Derived requirements are analyzed to ensure that the high-level requirements are not compromised.
* Failure condition response was determined consistent with safety-related requirements.
* Errors/deficiencies discovered during the Hardware Design Process are fed back into the system life cycle process for clarification and/or correction.

#### Transition Criteria for Exit from Implementation Process

Objective evidence (e.g., Meeting minutes, Action Items and Document Review Checklists) of Implementation Process activities are complete and verified. Implementation Process artifacts are produced, base-lined, reviewed, and under configuration management control including:

* Hardware Traceable To Hardware Requirements
* Target Integration Results
* VHDL Build and Load Control Procedure
* Preliminary Hardware Configuration Index

The following additional transition criteria are required:

* The design requirements are implemented in the hardware
* The hardware conforms to the hardware architecture
* The hardware implementation is traceable to the Design Description
* The hardware conforms to the VHDL Code Standards
* Errors or deficiencies discovered during the Hardware Implementation Process are fed back into either the Requirements Capture Process, the Hardware Design Process, or the Hardware Planning Process for clarification and/or correction

## Hardware Production Transition Process

In this process, manufacturing data, test facilities and general resources are examined to ensure availability and suitability for production. The production transition process uses the outputs from the implementation and verification processes to move the product into production.

### Process Objectives and Activities

Objectives of the Production Transition Process:

* A baseline is established that includes all design and manufacturing data needed to support the consistent replication of the hardware item.
* Manufacturing requirements related to safety are identified and documented and manufacturing controls are established.
* Derived requirements are fed back to the implementation process or other appropriate processes.
* Errors and omissions are provided to the appropriate processes for resolution.

Activities of the Production Transition Process:

* Manufacturing data are prepared from configured design data.
* Manufacturing data are checked for completeness and consistency with the configured design data.
* Any changes or improvements that are incorporated during the production transition process are evaluated to ensure they adhere to all product requirements, especially safety requirements. Any changes not compliant with customer or certification requirements are approved by the relevant parties.
* Manufacturing requirements pertaining to safety are explicitly defined so they can be controlled during the production process.
* Data required to develop acceptance test criteria are determined.
* Omissions or errors that are identified are provided to the appropriate process for resolution.
* An acceptance test is performed during this process. The acceptance test demonstrates that the manufactured, modified or repaired product performs in compliance with the key attributes of the unit on which certification is based. These key attributes are chosen using engineering judgment and are indicative that the product is capable of meeting the requirements to which the unit was developed.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware Process Assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Production Transition Process. Hardware Quality Engineers, Electrical Engineers, Mechanical Engineers, Electronic Technicians and the Hardware Librarian are involved in the System Integration process.

### Inputs

Inputs for the Production Transition Process include the hardware architecture, hardware, executable object code having completed S/W to H/W Integration, hardware architecture and hardware platform having completed Hardware Integration.

The HWCI, SWCI, System Verification Cases and Procedures and Verification Results, and Test Equipment are inputs to the QA Validation Testing Process. Electronic technician support may be required in setting up and conducting the tests.

### Outputs

The output of the Production Transition Process is an operational hardware system executing on the target hardware platform and a completed System Integration Review.

A validated System Verification Results Test Record is the output of the QA Validation Testing.

### Project Reviews

System Integration Review

The System Integration Review (SIR) is integrated into the Production Transition process. The SIR Checklist will be used during the review.

The Project Engineer conducts the SIR. When the SIR is held, the Project Engineer records the minutes or assigns someone to do so. The minutes will include a discussion of the results, agreements and disagreements reached during the review, updates to the project schedule and resource estimates, and action item assignments with estimated completion dates.

Representatives from Quality Assurance, Test Engineering, Manufacturing Engineering, Mechanical Engineering, and Hardware Engineering are invited to attend the SIR.

The review ensures the results of the integration process are complete and correct. If deficiencies are revealed during the review, corrective actions to resolve the deficiencies are fed back into the appropriate process.

Items to be considered at the SIR include, but are not limited to, the following:

* Hardware Addressing
* Memory overlays
* Missing components

System Verification Review

The QA Validation Testing phase begins with a Hardware Verification Review. A Review Checklist will be used to conduct the Review.

The Hardware process assurance Engineer conducts the review. The requirements-based test procedure is presented at the review. The procedure covers both normal range test cases and robustness test cases. The Project Engineer, Hardware and Hardware Engineers, and Manufacturing Test Engineers are invited to the review.

If deficiencies are revealed during the review, corrective actions to resolve the deficiencies are fed back into the appropriate process.

### Transition Criteria

#### Transition Criteria for Entry into Production Transition Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Implementation Process activities are completed and verified. Implementation Process artifacts are produced, base-lined, reviewed and under configuration management control including:

* Hardware Traceable To Hardware Requirements
* VHDL Build and Load Control Procedure

The following additional transition criteria are required:

* The hardware design is implemented
* The hardware conforms to the hardware architecture
* The hardware is traceable to the Design Description
* The hardware conforms to the VHDL Code Standards

Errors or deficiencies discovered during the Production Transition Process are fed back into the Requirements Capture Process, the Hardware Design Process, the Hardware Planning Process, or the Hardware Implementation Process for clarification and/or correction.

#### Transition Criteria for Exit from Production Transition Process

Objective evidence (i.e., Meeting minutes, Action Items and Document Review Checklists) of Code and Integration Process activities are completed and verified. Code and Integration Process artifacts are produced, base-lined, reviewed, and under configuration management control including:

* Target Computer Integration Results
* Hardware Build and Load Control Procedure
* Hardware Acceptance Test

The following additional transition criteria are required:

* The hardware is loaded into the target or host computer.
* Errors or deficiencies discovered during the Production Transition Process are fed back into the Requirements Capture Process, the Hardware Design Process, Hardware Implementation Process, or the Hardware Planning Process for clarification and/or correction.
* CM creates the Production Label in VSS.
* The hardware part number is released, showing the current version as the dash configuration (the initial configuration).
* CM and QA perform an independent build of the hardware and verify that the checksum produced is the same as that approved during test.
* CM and QA remove the old version of the hardware from the production hardware image directory.
* CM and QA place the newly released image in the production hardware image directory under the new hardware number.
* An ECO is issued to authorize the use of the new image.
* Production performs a test load of the image and verifies the checksum.

The following additional transition criteria are also required:

* Verifying that system requirements allocated to hardware are properly developed into high-level requirements.
* Verifying that high-level hardware requirements are properly developed into hardware architecture and derived requirements.
* Verifying that the hardware architecture is properly implemented.
* Verifying that the hardware implementation satisfied the hardware requirements.
* Verifying that the means used to meet these objectives are technically correct and complete.
* Verifying the developed Test Cases are appropriate and correct.
* Verifying the developed Test Procedures are appropriate and correct.

## Hardware Validation and Verification Processes

This section describes the validation process and the verification process. The validation process provides assurance that the hardware item-derived requirements are correct and complete with respect to system requirements allocated to the hardware item. The verification process provides assurance that the hardware item implementation meets all of the hardware requirements, including derived requirements.

The validation process discussed here is intended to ensure that the derived requirements are correct and complete with respect to the system requirements allocated to the hardware item through the use of a combination of objective and subjective processes. Validation may be conducted before or after the hardware item is available, however, validation is typically conducted throughout the design life cycle.

The verification process provides assurance that the hardware item implementation meets the requirements. Verification consists of reviews, analyses and tests applied as defined in the verification plan. The verification process should include an assessment of the results.

### Process Objectives and Activities

Objectives of the Validation Process:

* Derived hardware requirements against which the hardware item is to be verified are correct and complete.
* Derived requirements are evaluated for impact on safety.
* Omissions and errors are fed back to the appropriate processes for resolution.

Objectives of the Verification Process:

* Evidence is provided that the hardware implementation meets the requirements.
* Traceability is established between hardware requirements, the implementation, and the verification procedures and results.
* Acceptance test criteria are identified, can be implemented and are consistent with the hardware design assurance levels of the hardware functions.
* Omissions and errors are fed back to the appropriate processes for resolution.

Activities of the Validation Process:

* The derived hardware requirements that need to be validated are identified.
* Each requirement is validated at some hierarchical level by review, analysis or test.
* The review, analysis or test of each requirement is judged appropriate for validating the requirement, especially with respect to safety.
* The review, analysis or test results associated with the validation of each requirement are determined to be correct and discrepancies between actual and expected results are explained. When expected results are not pre-defined as may be the case for reviews and analyses, the results of the validation activity are consistent with the requirement, especially with respect to safety requirements.
* The derived requirements are evaluated for their impact on safety.
* The derived hardware requirements are evaluated for completeness with respect to the system requirements allocated to the hardware item. For the purposes of this process, a set of requirements is complete when all the attributes that have been defined are necessary and all the necessary attributes have been defined.
* The derived hardware requirements are evaluated for correctness with respect to the system requirements allocated to the hardware item. For the purposes of this document, a requirement is correct when the requirement is defined without ambiguity and there are no errors in the defined attributes.
* Traceability between the derived hardware requirements and the validation activities and results are established.
* Requirement omissions and errors are fed back to the appropriate process for resolution.

Activities of the Verification Process:

* Requirements that need a verification activity are identified. It is not intended that requirements are verified at every hierarchical level; requirements can be verified at a higher hierarchical level.
* Verification methods, such as tests, simulation, prototyping, analyses and reviews, are selected and performed.
* Traceability between requirements, implementation, and the verification procedure and results are established. Traceability is consistent with the design assurance level of the function performed by the hardware. It is not intended to require traceability to detailed components, such as resistors, capacitors or gates, unless required for safety considerations.
* Each requirement has been verified at some hierarchical level by review, analysis or test.
* The review, analysis, or test of each requirement is appropriate for verifying the requirement, especially with respect to safety requirements.
* The review, analysis, or test results associated with the verification of each requirement are correct and that discrepancies between actual and expected results are explained. When expected results are not pre-defined as may be the case for reviews and analyses, the results of the verification activity are consistent with the requirement, especially with respect to safety requirements.
* The results of the verification activities are documented.
* Omissions and errors are fed back to the appropriate process for resolution.

#### Elemental Analysis

Elemental analysis is utilized on projects involving complex hardware where the criticality levels are identified as Level A or Level B. Elemental analysis provides a measurement of the completeness of the hardware verification from a bottom-up perspective. Every functional element within the Functional Failure Path (FFP) is identified and verified using verification test cases. The analysis may also identify areas of concern that need to be addressed by other appropriate means.

Elemental analysis is used to show that FFPs are verified by associated verification test cases. Elemental analysis provides confidence and evidence that design errors are precluded by separating a complex implementation of the FFP into elements at the level that the designer generated it. This analysis method provides a measurement of the verification process to support the determination of verification coverage and completeness, and is most suited where the detailed design is visible and under configuration control.

##### Elemental Analysis Method

The elemental analysis method begins by defining a set of criteria to be applied in the analysis in consideration of the hardware design assurance level, the hardware technology and visibility of the details of the implemented hardware.

The criteria include identification and a definition of the elements at an appropriate level of the hardware design and the verification coverage to which each element should be verified. These criteria are then applied to the analysis of verification activities to determine whether the verification coverage completion criteria will be achieved by the planned verification. If the criteria will not be achieved, then each element being examined should be exercised by an appropriate set of stimuli and cause appropriate observable effects on the signals being monitored in the test.

The elemental analysis may be performed using a simulation to measure the completeness achieved, provided that the test procedures to be analyzed can be related to the elemental analysis criteria being applied and are those used for hardware functional verification credit. If the test procedures analyzed are derived from an in-circuit test of hardware or standalone prototype and are examined using a simulation, the test stimuli and expected results may be translated for the simulator provided that the translation process is checked for accuracy as a part of the elemental analysis. A simulator used to perform the elemental analysis should be shown to be able to correctly determine whether each type of element included in the implementation has met the analysis criteria.

##### Elemental Analysis Results Resolution

Elemental analysis may reveal hardware elements that were not verified, indicating either a need for additional verification process activities or perhaps a need to remove the untested element or mitigate any anomalous behavior that could result by architectural means.

###### Shortcomings in Verification Test Cases or Procedures.

Shortcomings may arise if the test cases do not test the elements in the hardware item. They may also arise if there are “don’t cares” in the functional requirements but the hardware item was appropriately designed to produce repeatable responses. Under these circumstances, the test procedures and cases should be supplemented or changed. Furthermore, the assertion of the test’s ability to verify its respective requirements should be reviewed.

###### Inadequacy in Requirements.

The requirements should be modified or additional derived requirements identified. Additional verification tests should then be developed for the new or revised requirements, executed and analyzed.

###### Unused functions.

The hardware item may contain functions that are not used in its target circuit application, such as unused sub functions within a library function or test structures used only for component-level acceptance tests. Such functions should either be shown to be isolated from the other used functions or shown to present no potential anomalous behavior that could have an adverse effect on safety. This could possibly be achieved by showing that the unused elements are positively deactivated either within the hardware or when installed. If the unused functions are to be used in some future application, the elemental analysis deficiency may be revisited at that time provided that such functions are identified as not being fully verified.

###### Elements of No Safety Consequence.

The consequence of anomalous behavior of the element can be bound and shown by analysis to not cause an adverse safety effect. These items should be resolved by recording the analysis bounding the consequence of anomalous behavior of the element.

##### Elemental Analysis Lifecycle Data

The elemental analysis lifecycle data output should:

* Identify the FFPs to be addressed by elemental analysis, and propose at what levels in the design hierarchy the elements are defined and how they are to be analyzed for verification adequacy, which are parts of the verification coverage completion criteria.
* Describe the methods and identify the FFPs addressed in the analysis and the levels in the design hierarchy at which the analysis was performed.
* Ensure that the traceability data shows the explicit relationship of the verification procedures to the elements in the elemental analysis.
* Identify the verification test cases and requirements added or modified as a result of the elemental analysis.
* State the level of the verification completeness achieved for the FFPs addressed by elemental analysis, including identification of the analysis discrepancies not resolved by modification to verification tests or requirements and the rationale for acceptability.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware process assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Hardware Verification Process.

### Transition Criteria

Transition criteria for the Hardware Verification Process are fully described in the Hardware Verification Plan.

## Hardware Configuration Management Process

The configuration management process is intended to provide the ability to consistently replicate the configuration item, regenerate the information if necessary, and modify the configuration item in a controlled fashion if modification is necessary. This section describes the objectives for hardware configuration management and activities that support these objectives.

### Process Objectives and Activities

Objectives of the Configuration Management Process:

* Configuration items are uniquely identified and documented.
* Consistent and accurate replication of configuration items is ensured.
* A controlled method of identifying and tracking modification to configuration items is provided.

Activities of the Configuration Management Process:

* Configuration items are uniquely identified, documented, and controlled. This may include, but is not limited to, hardware, design representations of hardware, tools, or other data items used for certification credit and baselines.
* Baselines are established.
* Problems are uniquely identified, tracked, and reported.
* Change control and traceability of changes are maintained. This requires that life cycle data identified in the plans are secure and retrievable.
* Archiving, retrieval, and release of configuration items are controlled.

Hardware Configuration Management is also responsible for:

* Hardware Configuration Management Records
* Problem Reports

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware process assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Hardware Configuration Management Process.

### Transition Criteria

Transition criteria for the Hardware Configuration Management Process are fully described in the Hardware Configuration Management Plan.

## Process Assurance

Process assurance ensures that the life cycle process objectives are met and activities have been completed as outlined in plans or that deviations have been addressed. This section describes the objectives for process assurance and the activities that support those objectives. There is no intent to impose specific organizational structures.

### Process Objectives and Activities

Objectives of the Process Assurance Process:

* Life cycle processes comply with the approved plans.
* Hardware design life cycle data produced complies with the approved plans.
* The hardware item used for conformance assessment is built to comply with the associated life cycle data.

Activities of the Process Assurance Process:

* Availability of hardware plans as specified in the planning process section of this document and as agreed to in the PHAC are ensured.
* Holding of reviews in compliance with the approved plans and tracking of resulting action items to closure are ensured.
* Detection, recording, evaluation, approval, tracking, and resolution of deviations from the hardware plans and standards are ensured.
* Satisfaction of the transition criteria of the hardware life cycle processes in compliance with the approved plans is ensured.
* An inspection is performed to ensure that the hardware item is built in compliance with its design data.
* Records of the process assurance activities, including evidence of assessment of completion of design activities, are produced.
* Where applicable, the applicant should ensure that the processes used by subcontractors are consistent with the hardware plans.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware process assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Process Assurance Process.

### Transition Criteria

Transition criteria for the Process Assurance Process are fully described in the Hardware Process Assurance Plan.

### Project Reviews

Hardware Conformity Review

The Hardware Conformity Review is held to obtain assurance that all Lifecycle processes are complete. The Hardware Quality Engineer conducts the review. The Hardware Quality Engineer assures that the Executable Object Code is controlled and can be regenerated. The Conformity Review Checklist will be used during the review.

## Certification Liaison Process

The purpose of the certification liaison process is to establish communication and understanding between the applicant and the certification authority throughout the hardware design life cycle to assist in the certification process. In addition, liaison activities may include design approach presentation for timely approval, negotiations concerning the means of compliance with the certification basis, approval of design approach, means of data approval, and any required certification authority reviews and witnessing of tests.

### Process Objectives and Activities

Objectives of the Certification Liaison Process:

* Resolve issues raised by the certification authority as a result of its reviews.
* Submit or make available other data or evidence of compliance requested by the certification authority.

Activities of the Certification Liaison Process:

* The PHAC, hardware verification plan and other requested data are submitted to the certification authority for review at a point in time when the effects of design changes on the program are minimal.
* Issues identified by the certification authority concerning the planning for the hardware aspects of certification are resolved.
* Agreement on the PHAC is obtained with the certification authority.
* Liaison with the certification authority during the design and certification cycle as outlined in the plan is continued and issues raised by the certification authority are resolved in a timely manner.

### Technical Interfaces

The Project Engineer, Hardware Engineer, Hardware Configuration Management Engineer, Hardware process assurance Engineer, FAA Certification Consultant and Systems and Equipment DER are involved in the Certification Liaison Process.

#### FAA Certification Consultant

A Certification Consultant will develop and implement systems, processes and documentation in order to provide the Applicant with the means to SHOW compliance with applicable 14 CFR's. The FAA Hardware Consultant's roles on this project are summarized below:

Serve as an advisor and/or reviewer for technical and process issues. The three sub-roles for the technical advisor/reviewer role are described below.

* Keeps up-to-date on the latest FAA policy and guidance related to hardware and certification by attending conferences, monitoring the FAA’s hardware web-site, and maintaining frequent communication with the certification authorities.
* Educates the project team on regulatory requirements and certification procedures.
* Strives to motivate the team to focus on safety.
* Assists the team in the interpretation of FAA policy and guidance related to hardware and certification. Further, helps the team apply those interpretations to the specific circumstances of their certification project.
* Helps certification authorities to understand the company’s installation, environment, product, project-specific certification issues, etc.
* Helps the development team to understand the underlying rationale behind DO-254, FAA policy and guidance, and regulations.
* Provides summary of lessons learned during certification projects.
* Serves as a resource for the company by being a corporate knowledge source regarding certification and by being aware of decisions made on other projects.
* Ensures that the hardware fits into the overall system and that there are no disconnections between the system requirements and hardware implementation.
* Strives to enforce consistency across multiple projects.
* Ensures strong ties between the system and hardware requirements.
* Encourages strong communication between systems, safety, hardware, and hardware engineers.
* Considers the overall safety implications of the system and the hardware.
* Reviews the safety analysis to ensure that the hardware level assigned is consistent with the safety assessment.
* Monitors the system and hardware development to make sure that safety assumptions are not adversely affected during the development effort.
* Ensures that hardware is mature, stable, and adequately verified prior to certification flight testing to ensure airworthiness of hardware as appropriate to the hardware criticality
* Ensures that there is good communications between QA and the DER.
* Ensures that QA is doing an effective job.
* Carries out planned and random reviews/audits to ensure compliance to objectives.
* Explaining and justifying to management the safety and regulatory requirements.
* Addressing problems that arise during the development effort.
* Clarifying misunderstandings related to DO-254 and FAA policy, guidance, and regulations.
* Works with teams early in the project to minimize certification issues.
* Explains to the FAA the issues that the development team encounters.
* Judges the proposals of the development team to determine if they will satisfy the regulations and/or DO-254 objectives.
* Serves as a facilitator between the FAA and the development team to help both sides understand each other.
* Researches new technology issues and how they relate to the DO-254 objectives.
* Serves on industry committees.
* Coordinates meetings between the project team and the Certification Authority.
* Develops strategies for Certification Authority coordination.
* Make presentations to the Certification Authority.
* Acts as a change agent to explain to the development team why certain things are important for certification and safety.
* Serves as coordinator between multiple DERs, product teams, and/or certification authorities.

#### Systems and Equipment DER

A Systems and Equipment DER, working in conjunction with the FAA Hardware Consultant, will be employed to perform reviews and audits in order to FIND compliance with 14 applicable CFR's (where authority has been delegated by the Certification Authority). The DER's roles on this project are summarized below:

* Ensures that there is tangible evidence to show that the objectives of DO-254, other applicable guidance, issue papers, and so forth are satisfied.
* Approves or recommends approval of hardware plans, data, and compliance findings by issuing 8110-3 forms against regulations.
* Ensures that the project plans are followed.
* Ensures that the processes established are yielding the results desired – i.e., making sure the development, verification, or integral processes are allowing the teams to satisfy the DO-254 objectives.
* Works closely with Hardware process assurance to ensure that processes and plans are being followed.
* Follows Orders 8110.105, 8110.49, 8100.8 and other applicable FAA policy documents related to the designee system.
* Ensures that all open problem reports have been evaluated to not negatively impact safety prior to certification.
* Performs routine reviews on projects that he/she will be approving
* Documents the review results in writing.
* Uses the FAA Hardware Review Job Aid to assist in conducting reviews.
* Informs the Certification Authority when reviews are planned and encourages Certification Authority involvement.
* Ensures that the project team addresses review findings/observations.
* Ensures that the ongoing verification process with project-level peers is being carried out properly.
* Prepares the development team for reviews by other designees or the Certification Authority.

# HARDWARE DESIGN LIFECYCLE DATA

In accordance with the assigned hardware control category per DO-254, the data in Table 6-1 and 6-2 will be created in the development of Passenger Counter system. See section 3.2 for descriptions of the document numbers in the following table.

| **Hardware Design Life Cycle Data** | **DO-254** | | **Note 1**  **Submit** | | **HW**  **Category** | | **Data Items**  **Passenger Counter FPGA** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hardware Plans | | 10.1 | |  | |  | |  |
| Plan for Hardware Aspect of Certification | | 10.1.1 | | S | | HC1 | | 800-PHAC-01  (this document) |
| Hardware Design Plan (HDP) | | 10.1.2 | |  | | HC2 | | 800-PHAC-01  (this document) |
| Hardware Validation Plan | | 10.1.3 | |  | | HC2 | | 800-HVVP-01 |
| Hardware Verification Plan | | 10.1.4 | | S | | HC2 | | 800-HVVP-01 |
| Hardware Configuration Management Plan | | 10.1.5 | |  | | HC2 | | 800-HCMP-01 |
| Hardware Process Assurance Plan | | 10.1.6 | |  | | HC2 | | 800-HPAP-01 |
| Hardware Design Standards | | 10.2 | |  | |  | |  |
| Requirements Standards | | 10.2.1 | |  | | HC2 | | 800-HRS-01 |
| Hardware Design Standards | | 10.2.2 | |  | | HC2 | | 800-HDS-01 |
| Validation and Verification Standards | | 10.2.3 | |  | | HC2 | | 800-HVVP-01 |
| Hardware Archive Standards | | 10.2.4 | |  | | HC2 | | 800-HRD-01 |
| Hardware Design Data | | 10.3 | |  | |  | |  |
| Hardware Requirements | | 10.3.1 | |  | | HC1 | | 800-HRD-01 |
| Hardware Design Representation Data | | 10.3.2 | |  | |  | |  |
| Conceptual Design Data | | 10.3.2.1 | |  | | HC2 | | 800-HRD-01 |
| Detailed Design Data | | 10.3.2.2 | |  | |  | |  |
| Top-level Drawing | | 10.3.2.2.1 | | S | | HC1 | | 800-HCI-01 |
| Assembly Drawings | | 10.3.2.2.2 | |  | | HC1 | | 800-HCI-01 |
| Installation Control Drawings | | 10.3.2.2.3 | |  | | HC1 | | 800-HCI-01 |
| Hardware/Software Interface Data | | 10.3.2.2.4 | |  | | HC1 | | 800-HRD-01 |
| Validation and Verification Data | | 10.4 | |  | |  | |  |
| Hardware Traceability Data | | 10.4.1 | |  | | HC2 | | 800-HTR-01 |
| Hardware Review and Analysis Procedures | | 10.4.2 | |  | | HC1 | | 800-HTP-01 |
| Hardware Review and Analysis Results | | 10.4.3 | |  | | HC2 | | 800-HTR-01 |
| Hardware Verification Test Procedure | | 10.4.4 | |  | | HC2 | | 800-HTP-01 |
| Hardware Verification Test Results | | 10.4.5 | |  | | HC2 | | 800-HTR-01 |
| Problem Reports | | 10.6 | |  | | HC2 | | Part of web development PR system |
| Hardware Configuration Management Records | | 10.7 | |  | | HC2 | | Part of web development PR system |
| Hardware Process Assurance Records | | 10.8 | |  | | HC2 | | CCB records, Checklists, Review Minutes, Audit Reports |
| Hardware Accomplishment Summary | | 10.9 | | S | | HC1 | | 800-HAS-01 |

Table 6- Passenger Counter FPGA Hardware Life Cycle Documents

*Data that should be submitted is indicated by an S in the Submit column. HC1 and HC2 data used for certification need not be submitted but should be available. Refer to DO-254 Section 7.3*

| **Hardware Design Life Cycle Data** | | **DO-254** | **Note 1**  **Submit** | **Hardware** **Category** | | **Data Items**  **Passenger Counter FPGA** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Hardware Plans | 10.1 |  | |  | |  | |
| Plan for Hardware Aspect of Certification | 10.1.1 | S | | HC1 | | 800-PHAC-01  (this document) | |
| Hardware Design Plan (HDP) | 10.1.2 |  | | HC2 | | 800-PHAC-01  (this document) | |
| Hardware Validation Plan | 10.1.3 |  | | HC2 | | 800-HVVP-01 | |
| Hardware Verification Plan | 10.1.4 | S | | HC2 | | 800-HVVP-01 | |
| Hardware Configuration Management Plan | 10.1.5 |  | | HC2 | | 800-HCMP-01 | |
| Hardware Process Assurance Plan | 10.1.6 |  | | HC2 | | 800-HPAP-01 | |
| Hardware Design Standards | 10.2 |  | |  | |  | |
| Requirements Standards | 10.2.1 |  | | HC2 | | 800-HRS-01 | |
| Hardware Design Standards | 10.2.2 |  | | HC2 | | 800-HDS-01 | |
| Validation and Verification Standards | 10.2.3 |  | | HC2 | | 800-HVVP-01 | |
| Hardware Archive Standards | 10.2.4 |  | | HC2 | | 880-HRD-01 | |
| Hardware Design Data | 10.3 |  | |  | |  | |
| Hardware Requirements | 10.3.1 |  | | HC1 | | 880-HRD-01 | |
| Hardware Design Representation Data | 10.3.2 |  | |  | |  | |
| Conceptual Design Data | 10.3.2.1 |  | | HC2 | | 880-HRD-01 | |
| Detailed Design Data | 10.3.2.2 |  | |  | |  | |
| Top-level Drawing | 10.3.2.2.1 | S | | HC1 | | 880-HCI-01 | |
| Assembly Drawings | 10.3.2.2.2 |  | | HC1 | | 880-HCI-01 | |
| Installation Control Drawings | 10.3.2.2.3 |  | | HC1 | | 880-HCI-01 | |
| Hardware/Software Interface Data | 10.3.2.2.4 |  | | HC1 | | 800-HRD-01 | |
| Validation and Verification Data | 10.4 |  | |  | |  | |
| Hardware Traceability Data | 10.4.1 |  | | HC2 | | 880-HTR-01 | |
| Hardware Review and Analysis Procedures | 10.4.2 |  | | HC1 | | 880-HTP-01 | |
| Hardware Review and Analysis Results | 10.4.3 |  | | HC2 | | 880-HTR-01 | |
| Hardware Verification Test Procedure | 10.4.4 |  | | HC2 | | 880-HTP-01 | |
| Hardware Verification Test Results | 10.4.5 |  | | HC2 | | 880-HTR-01 | |
| Problem Reports | 10.6 |  | | HC2 | | Part of web development PR system | |
| Hardware Configuration Management Records | 10.7 |  | | HC2 | | Part of web development PR system | |
| Hardware Process Assurance Records | 10.8 |  | | HC2 | | CCB records, Checklists, Review Minutes, Audit Reports | |
| Hardware Accomplishment Summary | 10.9 | S | | HC1 | | 800-HAS-01 | |

Table 6- Arinc 429 I/O FPGA Hardware Life Cycle Documents

*Data that should be submitted is indicated by an S in the Submit column. HC1 and HC2 data used for certification need not be submitted but should be available. Refer to DO-254 Section 7.3*

6.1 Relationship of Lifecycle Data to Other Data Defining The System

Configuration Management Records and Quality Assurance Records combine with the Lifecycle Data to form a complete system design data package. The following records are included:

* Planning Requirements, Design and Verification Data.
* Review Checklists from reviews identified in the Hardware QA Plan.
* Review Checklists from document reviews identified in the Hardware QA Plan.
* QA audit results as identified in the Hardware Product Assurance Plan.
* Project metrics as identified in the Hardware Product Assurance Plan.
* Problem reports as identified in the Hardware Configuration Management Plan.

# ADDITIONAL CONSIDERATIONS

This section describes the additional considerations. These include use of previously developed hardware, including references to applicable data to be reused, COTS usage, product service experience, and tool assessment and qualification or design assurance considerations for Level A or B functions.

## Use of Previously Developed Hardware

### 7.1.1 ARINC 429 I/O FPGA

The ARINC 429 I/O FPGA provides for transmitting and receiving of ARINC 429 data. The FPGA consists of four independent ARINC receivers and one ARINC 429 transmitter. The Transceiver interfaces to a micro controller via an 8 bit bidirectional data bus, 4 address lines and 4 control lines. The device is programmable to accept either analog or digital signals. The receivers are programmable for speed selection and automatic label recognition. The aircraft interfaces served by the FPGA remain unchanged; therefore the speed settings and label programming remain the same.

The ARINC 429 I/O FPGA part C800-1010-00 is currently used on earlier versions of the Passenger Counter and other systems for ACMEY co and will be reused in this design with no changes. The original DAL for this device was DAL level D.

#### 7.1.1.1 Product Service Experience Data Acceptability Criteria

The following sections discuss the relevance and acceptability of the service experience data.

##### Similarity – Application, Function, Operating Environment, and DAL

The ARINC 429 I/O FPGA was originally designed ACMEY Co engineering team in 1992. The FPGA was not developed using the processes defined in DO-254, since it did not exist at that time.

C800-1010-00 is the ACMEY Co. Part number for the ARINC 429 I/O FPGA. The service data used is for earlier version of the Passenger Counter I. The ARINC 429 I/O FPGA implements a standard ARINC 429 communications interface as used in the products listed. As a result, the previously mentioned application, installation and environment are directly applicable to the manner in which the ARINC 429 I/O FPGA is used in the Passenger Counter System. The original versions of the Passenger Counter are functionally identical and are interchangeable. The Passenger Counter II will be installed on the same aircraft as the original version.

The operational environment for the Passenger Counter II is the same as the Passenger Counter I. However, the Passenger Counter I was tested to DO-160D limits originally whereas the Passenger Counter II will be tested to the newer DO-160E standard.

##### Service Data Assessment

There are no known design errors or open problem reports for this part based on service data for the part which was used on the Passenger Counter I.

The service data was obtained from the Acmey Co. Reliability database used by the Acmey co. Repair and Overhaul Shop.

The following table lists the products built and shipped in which the ARINC I/O FPGA has been and is currently utilized. The “Total Units Shipped” number is 2100 as of June 2008:

|  |  |  |  |
| --- | --- | --- | --- |
| **Unit** | **Part Number** | **FPGAs per Unit** | **DAL Level** |
| Passenger Counter I | C800-1010-00 | 1 | C |

Table 7-1 Passenger Counter Products Using the ARINC 429 I/O

To calculate how long these units have been in operation, it is assumed that business jet units operate an average of 10 hours per day, 365 days per year and the average unit age is 5 years. At this rate, the units listed above have operated for a combined 38,325,000 hours.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Application** | **Units Shipped** | **FPGAs Shipped** | **Hours** | **Failures** |
| Passenger Counter I | 2100 | 2100 | 38,235,000 | 2 |

Table 7‑2 Failure Rate

The failure rate and MTBF of the ARINC 429 I/O can be calculated as follows:

Failure rate = hours/ failures=38,325,000/2= 1.91E-7

This failure rate satisfies the requirement for level C integrity (<1.0E-05).

The following table summarizes the Passenger Counter 1 ARINC 429 I/O FPGA failures reported by the Acmey Co. Repair and Overhaul shop.

| **Passenger Counter**  **Part Number** | **Units ARINC 429 FPGA Part No.** | **Passenger Counter  Serial No.** | **Date** | **Removed reason** |
| --- | --- | --- | --- | --- |
| C800-1010-00 | 1 | 220 | 2/2/2006 | Display failure |
| C800-1010-00 | 1 | 225 | 3/2/2006 | Display failure |

Table 7-3 Passenger Counter I ARINC I/O 429 FPGA Repair History

### 7.2.1 ARINC 429 I/O FPGA Re-verification

The configuration of this device will be documented as part of the Hardware Requirements Document for the passenger counter system and board level verification will be performed to demonstrate its correct operation in the passenger counter system. Hardware/ Software integration testing will also be performed to provide verification of this device in its new hardware environment. Traceability will be performed for the functions that this device performs to the system level requirements. All derived implementation will be analyzed and documented in the verification results document to see that there is no safety impact for unused functions of this device.

## 7.3 Use of Commercial-Off-The-Shelf (COTS) Components

The use of COTS components will be verified through the overall design process, including the supporting processes, as defined in this document. The use of an electronic component management process, in conjunction with the design process, provides the basis for COTS component usage.

## 7.4 SH-1 Issue paper compliance

The following sections address each aspect of the Issue Paper:

## Modifiable Devices

The devices used in this system are SRAM based and are loaded via a JTAG interface but only in the shop by the original manufacturer. Therefore the concerns related to Field-Loadable Hardware Logic, Option-Selectable Hardware Logic or User Modifiable Hardware Logic do not apply.

## 7.4.2 Certification Plan

A single PHAC (this document) will be generated to cover all ‘Programmed Electronic Hardware’.

## 7.4.3 Validation Processes

Validation is addressed by the Hardware Validation & Verification Plan document.

## 7.4.4 Verification Processes

Verification is addressed by the Hardware Validation & Verification Plan document.

## 7.4.5 Traceability

Traceability is addressed by the Hardware Validation & Verification Plan document.

### 7.4.6 Configuration Management

Configuration Index Documents are submitted in lieu of Top Level Drawings and will include the hardware design and verification environment.

### 7.4.7 Tool Assessment & Qualification

Not Applicable – Tool service history will not be used for credit. Each tool is checked by another tool or other independent means (section TBD refers).

### 7.4.8 Simple Electronic Hardware (SEH)

Not Applicable –both FPGAs will be treated as complex Programmed Electronic Hardware items for this program. Design assurance will be provided by a rigorous design life cycle rather than comprehensive testing.

### 7.4.9 Legacy Airborne Systems & Equipment Electronic Hardware

See section 7.2 above for previously developed FPGA usage.

### 7.4.10 Commercial Off-The-Shelf (COTS) Microprocessors

The PIC COTS Microprocessor will be used and the majority of the software testing will be performed on the target processor in order to verify the correct operation of this COTS device in its operating environment. A components management plan is in place at ACMEY CO for all COTS purchased parts to handle any revisions or modifications of this device by the manufacturer. The Errata for this device has been checked and there are no issues reported as of the date of this document.

### 7.4.11 Random Access Memory (RAM) based FPGAs

SRAM based FPGAs will be used in the system. Xilinx devices are SRAM based. An analysis of the operation and use of this system has been performed and due to the fact that is operated on the ground, there are very few atmospheric effects at this altitude. This has been reviewed by the system safety processes and the probability of failure on the ground is less than the 10-9 requirement for catastrophic systems, DAL A.

## 7.5 Tool Assessment and Qualification

Qualification of tools is required when processes of DO-254 are eliminated, reduced, or automated by the use of a hardware tool without its output being verified. The objective of the tool qualification process is to ensure that the tool provides confidence at least equivalent to that of the process or processes eliminated, reduced, or automated. This section lists all tools used to develop the hardware. Tools requiring qualification are identified and the appropriate qualification rationale provided.

Outputs of the design tools will be completely verified during the verification activities so that the integrity of the design does not depend upon the correctness of the design tool output alone.

### 7.5.1 Development Tools

Development tools that require qualification are those tools whose output is part of airborne hardware and can introduce errors. The following lists all development tools to be used on the program and identifies those tools that require qualification.

**Development and Verification Tools**

|  |  |  |
| --- | --- | --- |
| **Activity** | **Tool** | **Version** |
| Design Entry | Aldec Active HDL,  Mentor Graphics ViewLogic | 6.3  V7.0 |
| Synthesis | Xilinx ISE | 6.3g |
| Place & Route | Xilinx ISE | 6.3g |
| Simulation | Active HDL | 4.0 |
| Device Programming | Xilinx iMPACT | 6.3.0.1i |
| Source Revision Control | Visual Source Safe | 6.0 |

## 7.5.1.1 Qualification of Development Tools

RTCA/DO-254 requires that each development tool requiring qualification uses the same development processes for the tool which satisfy the same objectives as the hardware development process of the airborne hardware and that it is controlled in accordance with Control Category 1. This project does not use development tools requiring qualification.

* The HDL code is written using the Active HDL editor.
* For higher Level description the Active HDL Top-Level design entry editor will be used.
* This graphical entry tool used to describe functional blocks and the interconnections between them produces a HDL code, which will be reviewed by the designer.
* The HDL code representing the functions within the blocks is written using a HDL editor.
* The design flow includes the synthesis tool which takes the HDL code written by the designer and generates an output, which is a lower level representation of this code for the hardware Place & Route tool which fits the design into the physical component, by generating the programming file.
* The programming file is downloaded into the hardware, configuring the physical component, which will be tested.
* Synthesis output will be analyzed and will be regarded as an intermediate step to produce the input for the fitting process.
* The fitting process also produces the HDL timing model which will be used during the simulation.

The models used to simulate the representative functions will be analyzed using the results of target testing.

### 7.5.2 Verification Tools

Verification tools that require qualification are those tools that cannot introduce errors, but may fail to detect them. The following lists all verification tools to be used on the program and identifies those tools that require qualification. Tool descriptions, functionality, usage, and their role in the Lifecycle process are fully described in the applicable Plans.

|  |  |  |
| --- | --- | --- |
| Tool Name | Tool Description | Qual Required |
| PRMS | Problem Reporting Management System | No |
| RTMS | Requirements Traceability Management System | No |
| AIMS | Action Item Management System | No |
| DRMS | Document Review Management System | No |
| VSS | Hardware Version Control Management System | No |
| MS Word | Lifecycle Document Preparation | No |
| MS Excel | Requirements Traceability Matrix Preparation | No |
| MS PowerPoint | Meetings and Presentations | No |
| MS Project | Project Schedules and Milestones | No |
| MS Visio | Flow Chart and Diagram Program | No |
| ALDEC Active-HDL EE | Place and Route | No |
| ALDEC Active-HDL EE | Compilation / Simulation | No |
| ALDEC Active-HDL EE\* | Bench Testing | No |
| ALDEC Active-HDL EE\* | Statement and Branch Coverage | No |
| ALDEC Active-HDL EE\* | Toggle Coverage | No |
| ALDEC Active-HDL EE\* | Expression Coverage | No |
| ALDEC Active-HDL EE | Visualization Tools | No |

\* This tool has outputs which are examined, or which feed into operations whose outputs are examined or this tool is used as a coverage tool for elemental analysis which does not require qualification per DO-254 section 11.4.1(4). Therefore, no tool qualification is required.

# ALTERNATIVE METHODS

This section describes any alternative methods proposed for the program, which are either not described in this document or are to be applied in a manner other than as described in this document. Justification for why the alternative method is acceptable should be provided. There will be no alternative methods used on this project.

# CERTIFICATION SCHEDULE

This section describes the means that will be employed in order to provide the customer and/or certification authority with visibility of the activities of the lifecycle processes. This section also provides an overview of the Web-based systems used to show compliance.

The master schedule is maintained by the Project Manager. An excerpt is provided below:

|  |
| --- |
| DO254_Schedule |

The following milestones are defined in the master schedule and provide the certification authority with the means to plan their project involvement:

* Stage of Involvement #1: Planning Review
* Stage of Involvement #2: Development Review
* Stage of Involvement #3: Verification Review
* Stage of Involvement #4: Final Review

## Project Schedule

Project Milestones

| **Project Milestone** | **Plan Completion Dates** | **Previous Date Reported** | **Revised or Actual** |
| --- | --- | --- | --- |
| - Planning Review (SOI#1) |  |  |  |
| - Requirements Review |  |  |  |
| - Preliminary Design Review |  |  |  |
| - Critical Design Review (SOI#2) |  |  |  |
| - Implementation Review |  |  |  |
| - System Integration Review |  |  |  |
| - System Verification Review (SOI#3) |  |  |  |
| - Conformity Review (SOI#4) |  |  |  |

Customer Deadlines (Red Label, Black Label, Documentation)

| **Type** | **Date Due** | **Qty** | **Completed** |
| --- | --- | --- | --- |
|  |  |  | checkmark |
|  |  |  |  |
|  |  |  |  |

**Regulatory Certifications Required** (TSO, STC, PMA, FCC, Etc.)

| **Type** | **Date Due** | **Completed** |
| --- | --- | --- |
|  |  | checkmark |
|  |  |  |
|  |  |  |

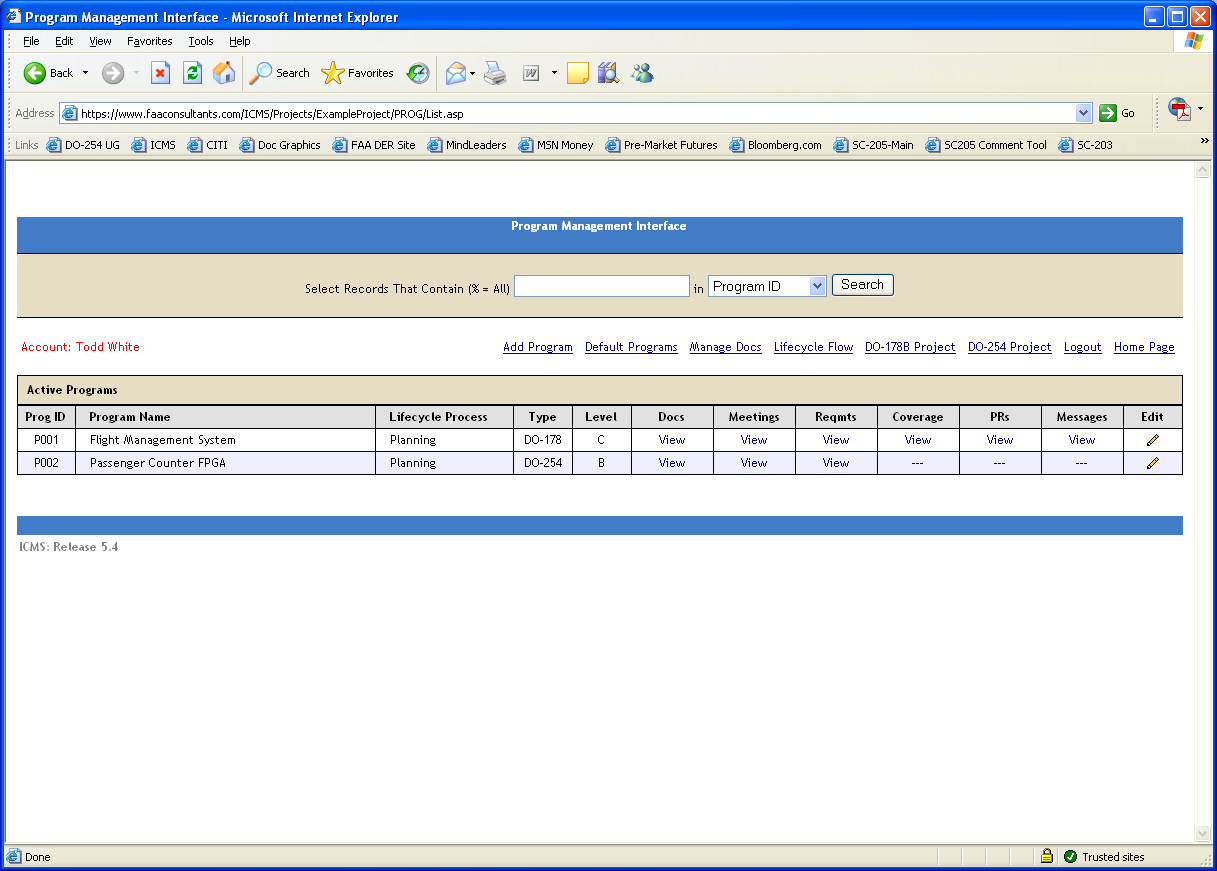
## Certification Authority Web Interface

The Certification Authority Web Interface was developed to provide visibility to the customer and/or Certification Authority. The system allows secure access to safety-critical hardware projects and related artifacts and objective evidence. This Web interface provides secure access to the Project-Level Integrated Compliance Management System.



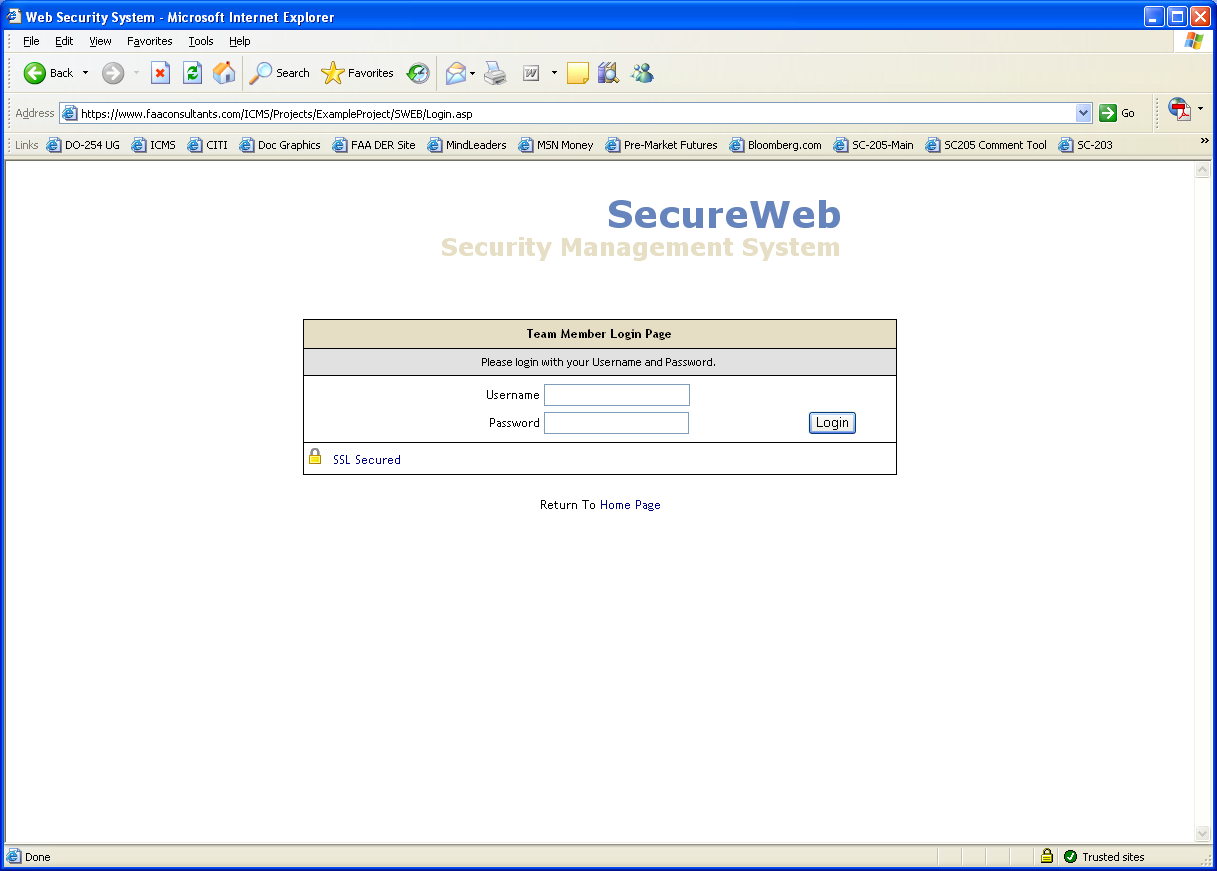
## Project-Level Integrated Compliance Management System

The Project-level Integrated Compliance Management System is used as the interface between the Project Team, Customer, and/or the FAA. The information in this system is applicable to a particular FAA hardware project. This Web-based system is comprised of a SecureWeb Management System, Problem Reporting Management System, Document Review Management System, Meeting and Action Item Management System, Requirements Traceability Management System, and Coverage Analysis Management System. All systems are specifically developed to show compliance with the objectives of DO-254.



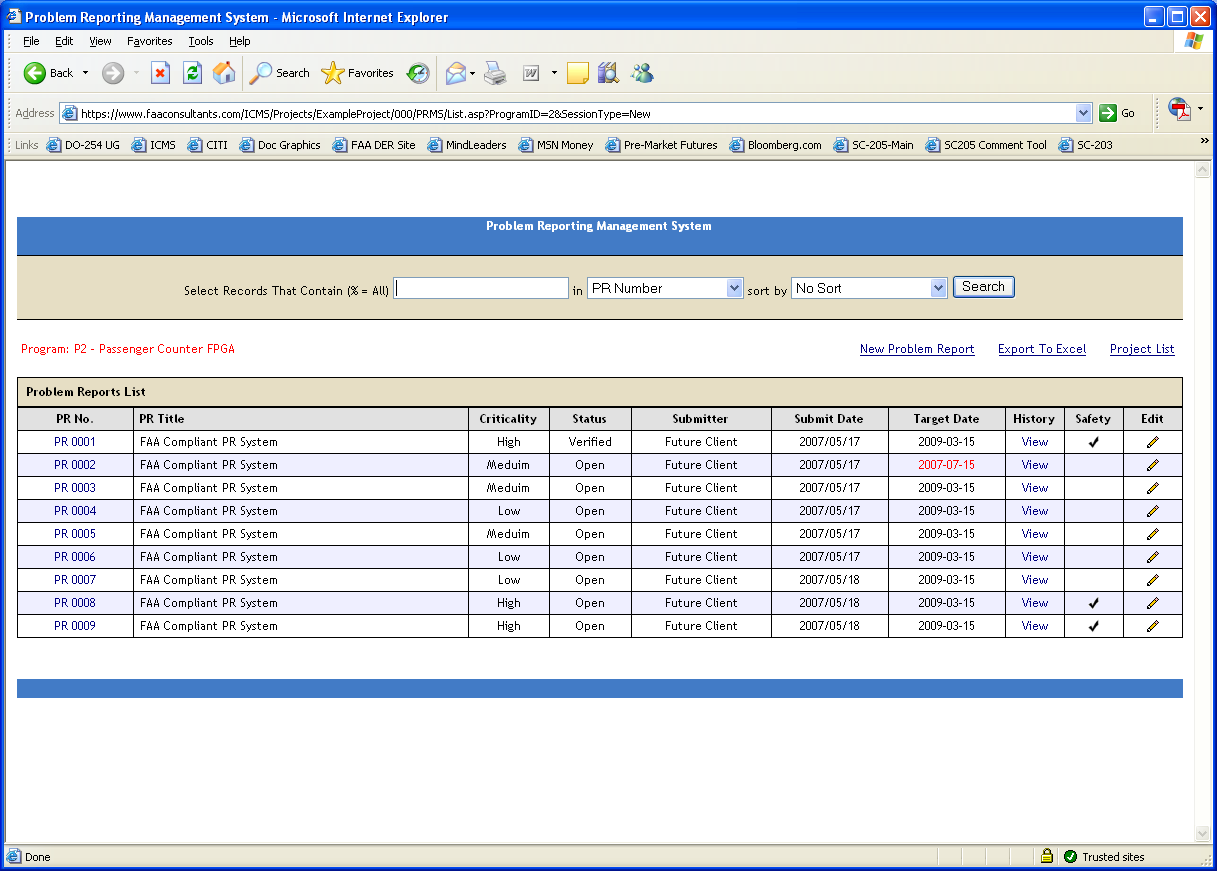
### SecureWeb Security Management System

The SecureWeb Security Management System generates a unique database record for each team member. The system allows team members to login and logout. The user benefits from being able to sign on, because it associates content they create with their personal account and allows permissions to be set for their roles.



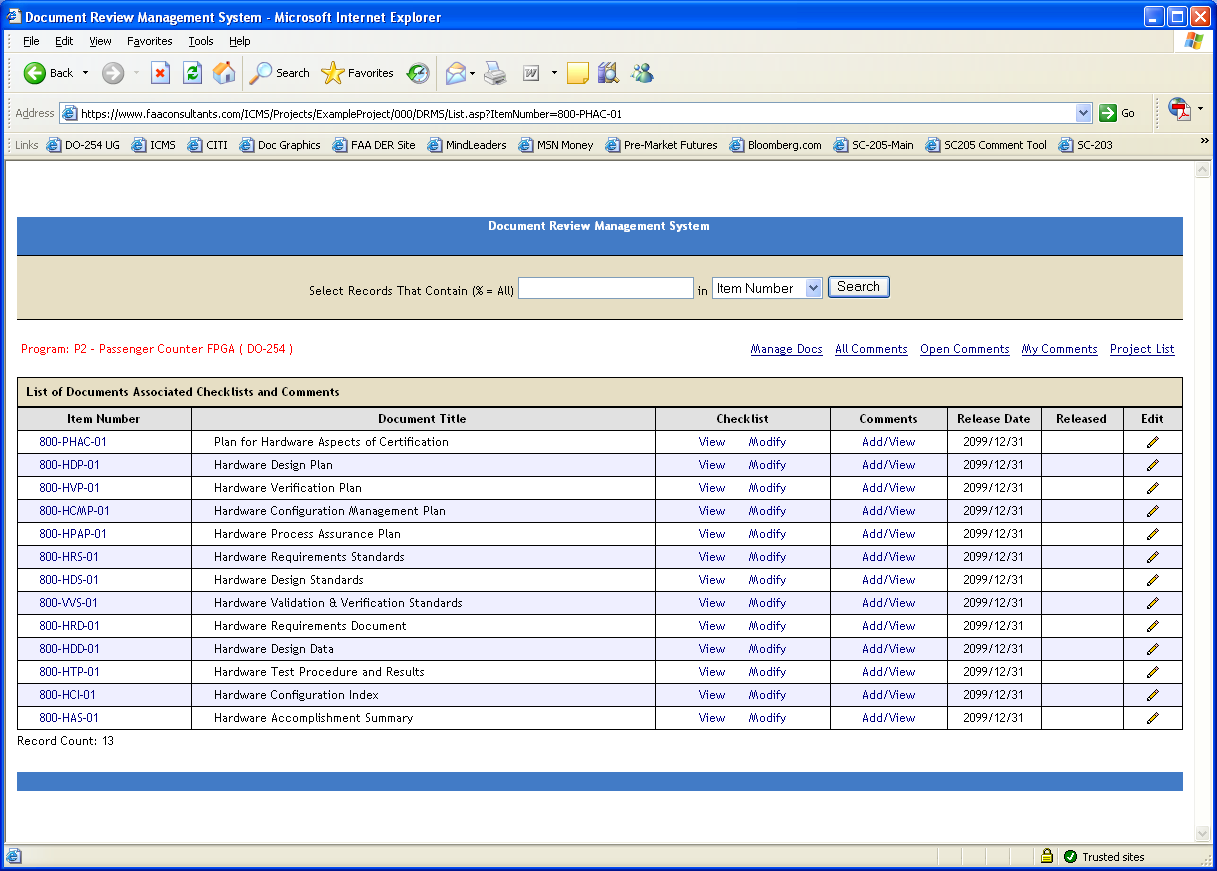
### Problem Reporting Management System

The Problem Reporting Management System generates a unique database record for each problem / improvement request. A Problem Report can be created by anyone. Automatic email notification of Problem Report adds modifications and closures. Safety-related Problem Reports are flagged. Status updates and assignments are restricted / secure.



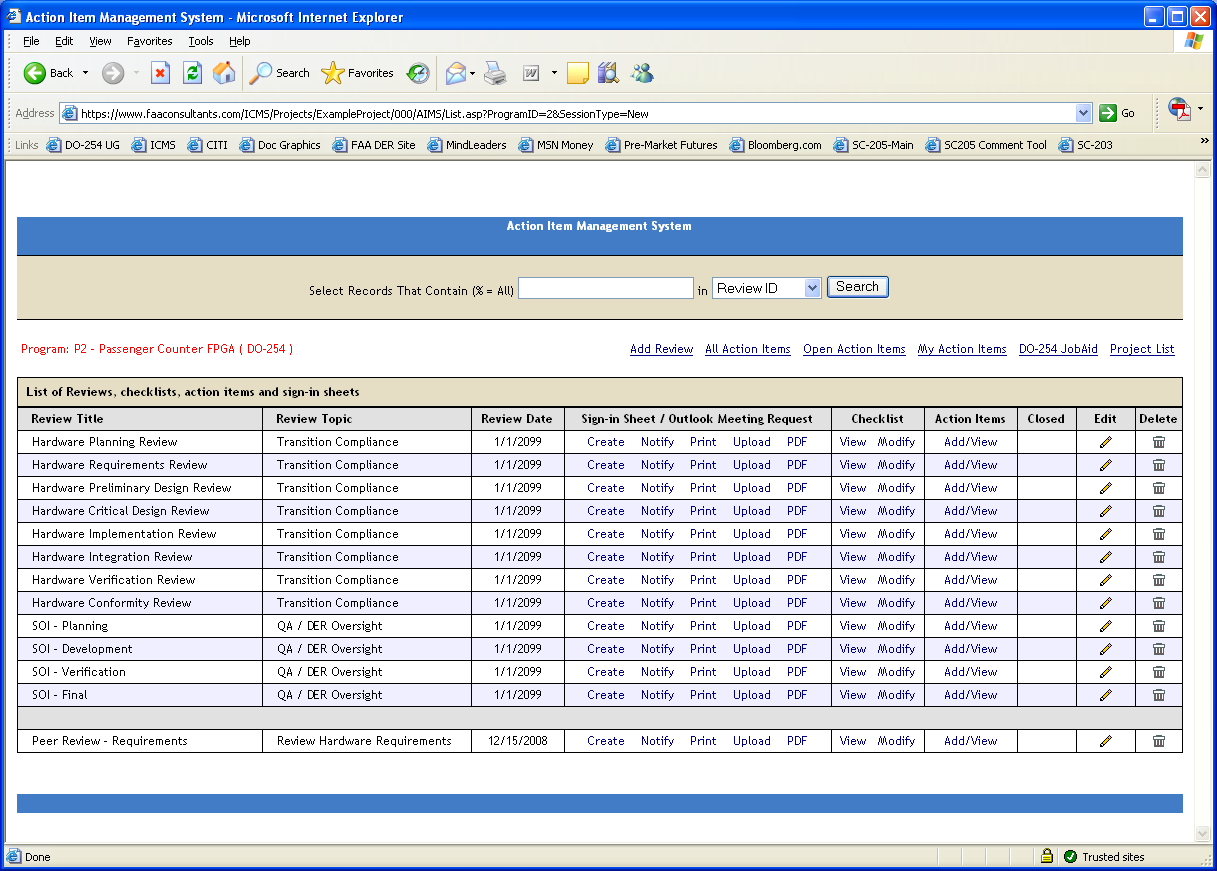
### Document Review Management System

The Document Review Management System generates a unique database record for each document, provides a hyperlink to the document, automatically creates a checklist addressing all DO-254 Section 10 objectives, and creates an action item sub-system for recording inputs from individuals reviewing the document and provides email notification.



### Action Item Management System

The Action Item Management System generates a unique database record for each meeting, automatically creates checklists addressing DO-254 objective, creates a list of documents required for the review, and creates an attendees list and an action item sub-system for recording and managing action items.



### Requirements Traceability Management System

The Requirements Traceability Management System generates a unique database record for each requirement. Requirements definition is from the System Level to the High Level Hardware Requirements to the Low Level Hardware Requirements to the Hardware Module to the Test Cases. Exportable System Requirements are Document Matrix, Hardware Requirements Document Matrix, Hardware Design Document Matrix and Top Down / Bottom Up Traceability Matrix.

