THESIS

FUEL TANK INERTING SYSTEMS FOR CIVIL AIRCRAFT

Submitted by

David E Smith

College of Electrical and Computer Engineering

In partial fulfillment of the requirements

For the Degree of Master of Science

Colorado State University

Fort Collins, Colorado

Fall 2014

Master's Committee:

Advisor: Ron Sega

Peter Young
Edwin Chong
Robert France

ABSTRACT

FUEL TANK INERTING SYSTEMS FOR CIVIL AIRCRAFT

This thesis examines and compares a variety of methods for inerting the fuel tanks of civil transport aircraft. These aircraft can range from the 50-seat Bombardier CRJ-200 to the 525-850 seat Superjumbo Airbus A380 and can also include airliner-based VIP aircraft such as the Boeing Business Jet (BBJ) or executive-class aircraft such as the Learjet 85.

Three system approaches to fuel tank inerting are presented in this paper with the intent of providing senior systems engineers and project managers a comparative requirements analysis and a thorough analysis of the different levels of documentation effort required for each rather than performing a simple technical trade-off study to determine which system architecture is the lowest weight or perhaps has the least parts count.

When choosing a system architecture, requirements analysis is often overlooked and documentation workload is brushed aside in favor of purely technical analyses. This thesis paper aims to provide examples of why the non-technical analyses are also important in good systems engineering.

AUTOBIOGRAPHY

I began my avionics career as an aircraft electrical technician for the U.S. Navy in 1975. After an honorable discharge I continued as a tech, then manager and finally Director of Avionics for Executive Jet Aviation (now NetJets). In 1997 I moved to Honeywell Aerospace (Glendale, AZ) as an avionics systems engineer where I worked on a variety of new aircraft and flight control certification programs. I left Honeywell in 2005 to pursue an independent consulting business in program management of airborne software development. Most recently (July 2014) I finished 5 ½ years as an equipment manager & systems engineer with Parker Aerospace's Fluid Systems Division in Irvine, CA. Presently I am Director of Programs at Phoenix Logistics of Tempe, AZ which manufactures electronic assemblies and systems for military aircraft.

- Avionics Engineering Technology: Columbus State – 1984
- Electrical & Computer Engineering: Franklin University – 1995
- MBA: Arizona State University – 2001
- Project Management: University of Phoenix – 2005
- MS Systems Engineering: Colorado State – December 2014
- Project Management Professional – June 2008
- Certified System Engineering Professional – January 2014

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

On 17 July, 1996 a Boeing 747, Flight TWA 800, exploded in mid-air about 12 minutes after take-off from John F. Kennedy airport. The accident investigation, conducted by the Federal Bureau of Investigation and the National Transportation Safety Board (NTSB), concluded that instead of the suspected act of terrorism the incident was caused by the ignition of hot fuel vapors in the aircraft's central fuel tank. According to the NTSB, the aircraft had been sitting on hot pavement for a few hours before the flight which was plenty of time to warm the central nearly empty, bottom-mounted fuel tank to the temperature necessary for the fuel to vaporize. Once the fuel tank was full of warm fuel/air vapors all that was necessary was a source of ignition, likely a short in the fuel quantity system electrical wiring, for the center fuel tank to explode. All 230 persons on board perished in the catastrophe.

A 1999 Department of Transportation & Federal Aviation Administration report (DOT/FAA/AR-99/73)[1] studied 13 worldwide accidents involving fuel tank explosions during the period from 1966 to 1995. The authors ran 9999 Monte Carlo iterations of random selections, finding a best estimate of 9 lives per year would be saved if the air transport fleet were equipped with fuel tank inerting. An important assumption in the report is that all fuel tank explosions would have been prevented by the use of onboard inerting systems (unless fuel tanks are severely ruptured and nitrogen lost).

[1] DOT/FAA/AR-99/73: A Benefit Analysis for Nitrogen Inerting of Aircraft Fuel Tanks Against Ground Fire Explosion, Ray Cherry and Kevin Warren

According to a FAA Fact Sheet[2], the TWA 800 accident "fundamentally altered the assumptions held by the FAA, airlines, manufacturers, and the NTSB. Prior to the TWA 800 accident, the prevailing philosophy among the world's aviation experts was that minimizing ignition sources was the best way to avoid a fuel tank explosion. However, the ignition source for the TWA 800 accident remains unknown." The Fact Sheet continues, declaring that now "The FAA is pursuing the right safety solution: eliminate ignition sources and reduce the flammability of the tank."

The TWA 800 incident prompted the NTSB to recommend new rules be enacted to reduce the likelihood of fuel tank explosions on commercial transport aircraft (airliners). Following this recommendation the Federal Aviation Administration (FAA) created Amendment 25-102 to Federal Aviation Regulation (FAR) 25.981 Fuel Tank Ignition Prevention, which requires "minimization of the formation of flammable vapors in the fuel tanks"[3]. In essence, this amendment required a Fuel Tank Inerting System (FTIS) on all newly designed transport category aircraft, not including those carrying only cargo.

The most practical method for reducing the flammable vapors in an aircraft's fuel tank is to replace the oxygen in the space above the fuel's surface, known as ullage, with a non-flammable gas such as Nitrogen. In a 1971 report[4] produced by the National Aviation Facilities Experimental Center (NAFEC), studies of nitrogen inerting requirements for the safety of aircraft fuel tanks from the previous 30 years were examined. These studies had been performed by a wide variety of entities, including

[2] FAA Fact Sheet – Fuel Tank Safety, 29 June 2006

[3] FAA Advisory Circular 25.981-2A

[4] FAA-RD-71-42: Inerted Fuel Tank Oxygen Concentration Requirements

the Boeing Aircraft Company, the Department of the Interior's Bureau of Mines, University of California, Naval Research Laboratory, Wright Aeronautical Development Center, Royal Aircraft Establishment and Convair Aircraft Company. The NAFEC report describes the trade-off between two inerting gases, Carbon Dioxide (CO_2) and Nitrogen (N_2): CO_2 has a higher volumetric heat capacity (Btu/ft^3) so it is better at quenching flames than N_2 but the purpose of a fuel tank inerting system is to prevent the occurrence of ullage ignition and consequently the flames will not exist. Other observations made in the report were that although less CO_2 is required to produce a nonflammable ullage, CO_2 is heavier, requires a heavier compression container, has icing problems when released and is more soluble in fuel which can cause lower engine performance due to fuel dilution.

A later NAFEC report[5], released in 1972, describes the results of flight testing a liquid nitrogen inerting system onboard a FAA-operated DC-9 commercial transport plane. The aircraft was thoroughly instrumented so that ullage pressures and oxygen concentrations could be measured at all locations within the wing fuel tanks and the center fuel tank, during all flight phases. The inerting system was able to maintain a positive pressure in all three fuel tanks (left wing, center, and right wing) which, even at the ullages' peak oxygen concentrations, kept all tanks well below the level considered inert and unable to support combustion.

In an FAA technical paper authored by William Cavage and Robert Morrison of the FAA's William J. Hughes Technical Center, Fire Safety Branch in Atlantic City[6], an

[5] FAA-RD-72-53: Performance of a DC-9 Aircraft Liquid Nitrogen Fuel Tank System

[6] Development and Testing of the FAA Simplified Fuel Tank Inerting System, W.M. Cavage & R. Morrison

On-Board Inert Gas Generation System (OBIGGS) was studied as an alternative to the more weight-intensive method of utilizing liquid nitrogen. The OBIGGS method was made possible by newly developed Hollow Fiber Membrane (HFM) technology which separates the Nitrogen and Oxygen molecules from a stream of ordinary atmospheric air. After removing most of the Oxygen from the air stream the remaining Nitrogen-rich air is sent to the fuel tank(s) to create an inert ullage. The HFMs are bundled tightly together inside a metal canister called an Air Separation Module (ASM) which is then connected to an air source. Figure 1 is a simplified pictorial of an ASM, presented by Cavage & Morrison at an International Fire and Cabin Safety Research Conference, held in Lisbon, Portugal in 2004[7].

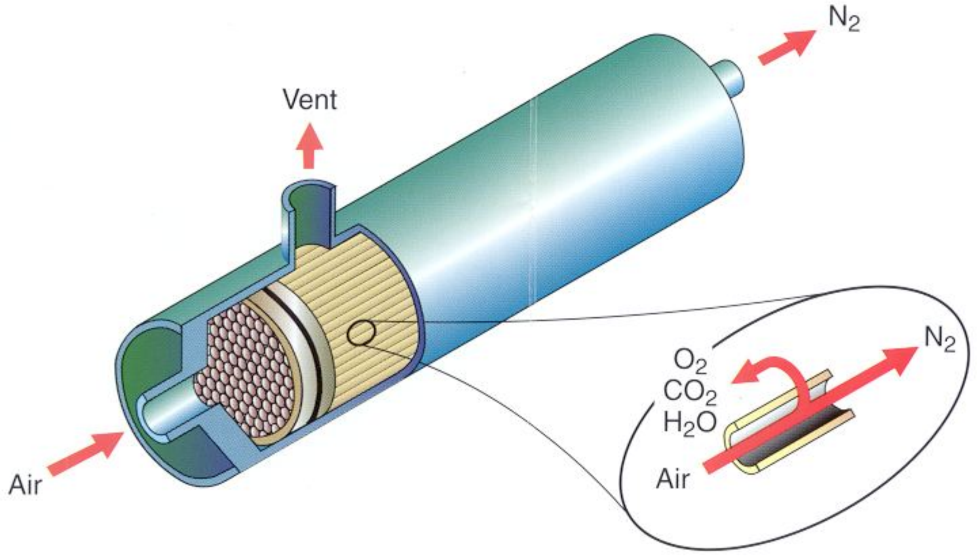


Figure 1: Air Separation Module

The Cavage & Morrison technical paper provides summary descriptions of a ground test installation aboard a decommissioned Boeing 747SP along with dynamic in-

[7] Development and Testing of the FAA Simplified Fuel Tank Inerting System, a PowerPoint presentation by W.M. Cavage & R. Morrison

flight testing of an Airbus-supplied A320 and the NASA 747 Shuttle Carrier Aircraft (SCA), shown in Figure 2.

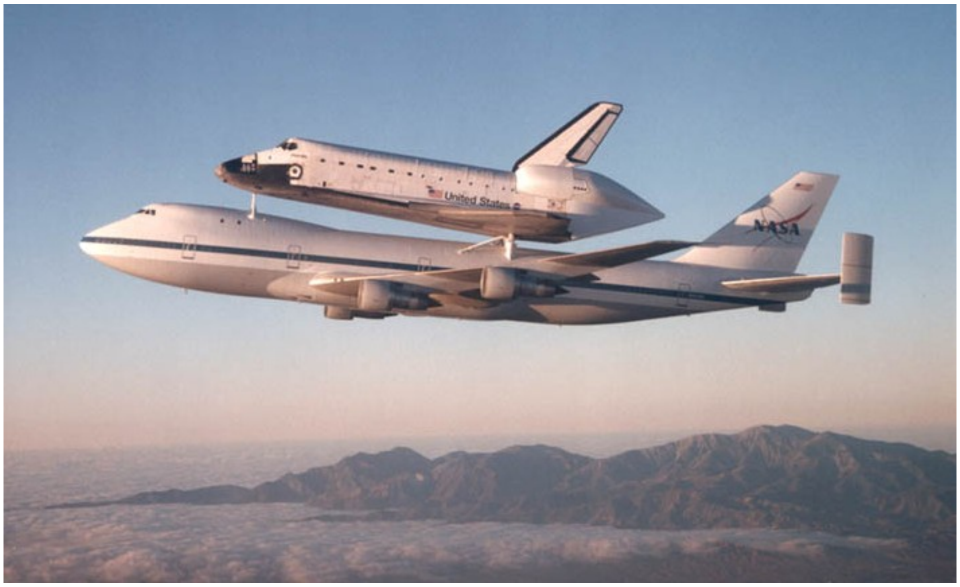


Figure 2: NASA Shuttle Carrier Aircraft

The inerting system as installed for ground testing is shown in Figure 3. This view is from underneath, looking up at the belly of the aircraft where the installing engineers were fortunate to find adequate space available for the entire system. The system installed in the NASA 747 SCA was virtually the same as that installed in the ground test article and employed the same instrumentation.

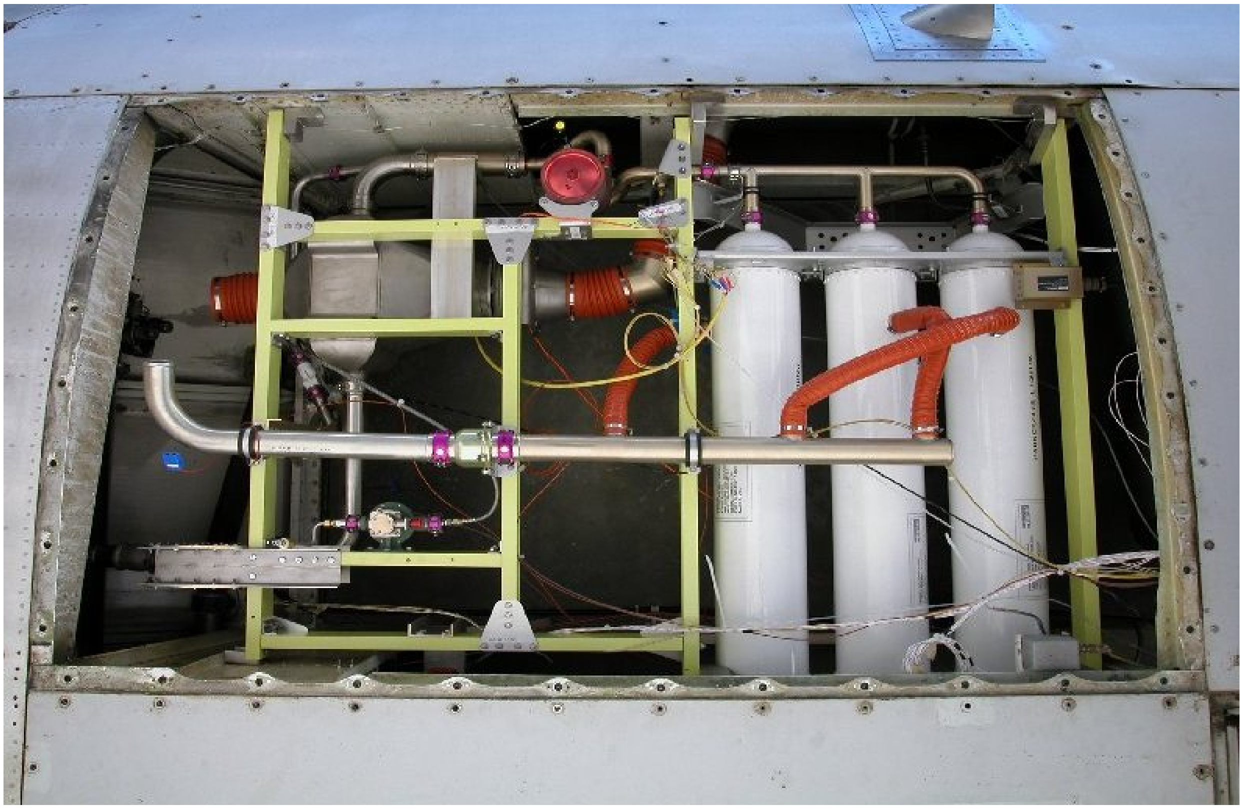


Figure 3: OBIGGS Installed in Boeing 747 SP Ground Test Article

A very detailed description of the NASA 747 SCA inerting system installation, the flight tests performed, and the test results were published in an FAA report, also authored by Cavage & Morrison along with Michael Burns and Steven Summer[8]. A similar FAA report[9], with Burns, Cavage, Morrison, and Richard Hill as authors, covers the same type and depth of information for the A320 flight tests.

On the Airbus A320 flight test vehicle, the inerting system was installed in the cargo bay, shown in Figure 4.

[8] DOT/FAA/AR-04/41: Evaluation of Fuel Tank Flammability and the FAA Inerting System on the NASA 747 SCA

[9] DOT/FAA/AR-03/58: Flight-Testing of the FAA Onboard Inert Gas Generation System on an Airbus A320

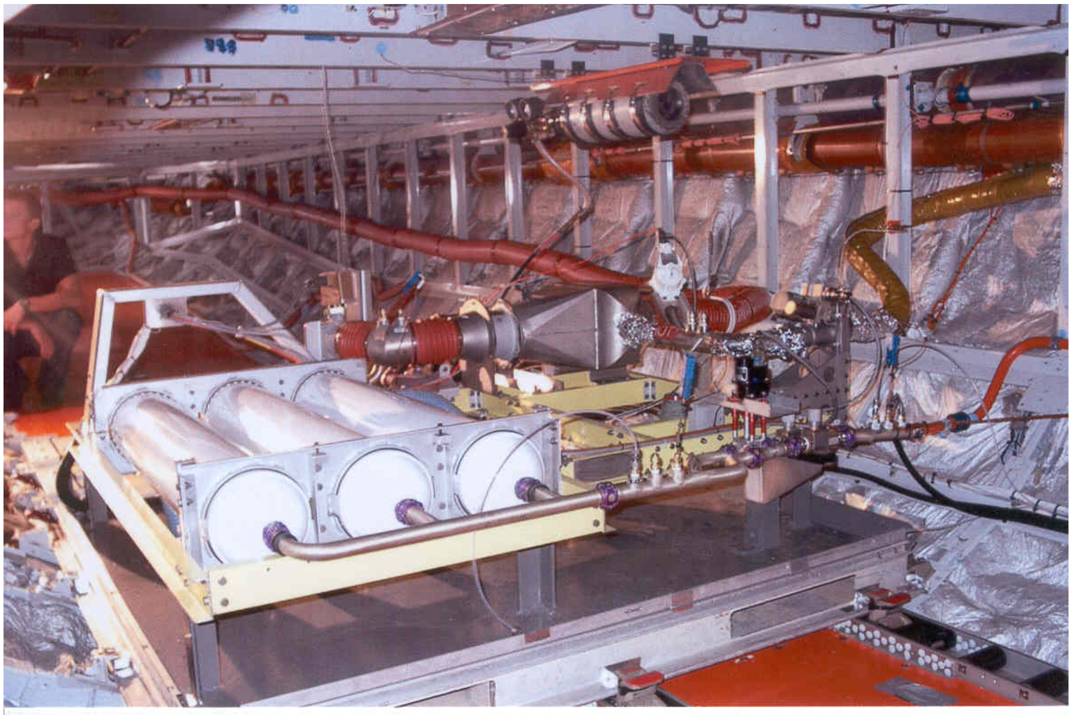


Figure 4: OBIGGS Installed in Airbus A320 Flight Test Vehicle

All three installations utilized main engine bleed air for the ASM's atmospheric air stream. Ground testing validated the OBIGGS concept but ASM performance varied greatly with temperature, as warm HFMs separate out the Oxygen molecules more efficiently. Flight tests of both the A320 and the 747 SCA also validated the OBIGGS and it was noted that pressure altitude had a much larger effect on bleed air consumption than was expected. The paper suggested more research of HFMs would be necessary "to determine what changes in system design or operational methodology would best reduce the bleed air flow and the associated cost".

Military aircraft have long utilized the onboard storage method, typically with LN_2 or Halon. In a 1987 SAE Technical Paper[10] written for an Aerospace Technology

[10] SAE Technical Paper Series 871903: OBIGGS For Fighter Aircraft

Conference and Exposition, the recently-developed ASM technology (OBIGGS) was compared with existing onboard storage FTISs similar to those used on the F-15 fighter aircraft. In the technical paper, R.G. Clodfelter of the Aero Propulsion Laboratory at Wright-Patterson Air Force Base in Ohio, along with C.L. Anderson and W.L. Vannice of the Boeing Military Airplane Company in Seattle, Washington found the onboard storage method to remain the best for dealing with the typical fighter's ability to make massive altitude changes, which was assumed to be a descent of 60,000 feet in 54 seconds. During a descent an aircraft's fuel tanks' inertness become spoiled by atmospheric air via the fuel venting system. As the aircraft descends, atmospheric pressure outside the wing tanks increases and the fuel tanks "inhale" air containing 21% oxygen which quickly brings the ullage above the flammable level. To meet a fighter aircraft's need for inerting gas during such a maneuver a pure OBIGGS system would need to be extremely oversized, with many ASMs connected in parallel.

Clodfelter, Anderson and Vannice suggested a hybrid OBIGGS/Onboard Storage system that would use a turbo-compressor in conjunction with the OBIGGS to store, during ascents and level cruising, enough compressed NEA to keep the fuel tanks inert during descents. A commercial airliner's typical descent rate is a fraction of a fighter aircraft, but a thorough FTIS sizing study may determine that adding a turbo-compressor and a small storage tank may allow the removal of a few ASMs from the proposed system, especially if lighter weight compressors and tanks are someday developed.

PROBLEM STATEMENT

With an amended FAR requiring the fuel tanks on newly designed airliners be made inert, to prevent tragedies such as TWA 800, the airline manufacturers have been challenged to choose the optimum FTIS for their particular aircraft. Unfortunately, adding such a system also adds weight and cost – each of which can be considered the bane of a successful aircraft design.

The additional weight of an FTIS can easily be measured by totaling the system's component weights plus any necessary aircraft physical interfaces such as mounting points. The cost of adding an FTIS is not so easily determined and is always more than just the cost of components, due to the additional documentation. Such documents include those typically produced for every system on board a transport category aircraft: system safety analyses; requirements databases at the manufacturer, system supplier, software developer, and component supplier levels; proof of requirement traceability and compliance evidence; individual component environmental qualification testing procedures and results; system environmental qualification testing procedures and results; proof of compliance with the Radio Technical Commission on Aeronautics' (RTCA) DO-178B and DO-254 processes for software and complex electronic hardware development and their related audits; test procedures and results for integrating the system with the aircraft; proof of compliance with the Society of Automotive Engineers' ARP-4754A process for developing systems for airborne use; and a variety of certification documents determined by each aircraft manufacturer. All of the documentation involved with developing an FTIS is also subject to review and approval at one level above the aircraft manufacturer, by the certification authorities, which is the FAA or Transport Canada in North America, the Civil Aviation Authority in the UK and the European Aviation Safety Agency (EASA) in the European Union.

When the weight of the paper [documentation] equals the weight of the airplane, only then you can go flying.

— attributed to Donald Douglas[11]

With the uncertainty in arriving at a cost estimate for developing an FTIS, given the variables per aircraft manufacturer and various certification environments, this thesis paper will focus on system complexity as a basis for comparing costs. Differing contractual requirements is another justification for this approach, as Airbus and Boeing may prefer to provide all aircraft flight testing equipment while Bombardier may require the system supplier to also foot the bill for expensive oxygen measuring equipment, for example.

[11] Great Aviation Quotes: http://www.skygod.com/quotes/flyingjokes.html

A COMPARISON OF THREE FTIS ARCHITECTURES

As noted in the Introduction, the most practical method for reducing the flammable vapors in an aircraft's fuel tank is to replace the oxygen in the ullage with an easily obtained non-flammable gas such as Nitrogen. This can be accomplished by either distributing the Nitrogen gas to the fuel tanks from storage tanks carried onboard the aircraft or from an onboard Nitrogen generator.

For the storage onboard method, Nitrogen is generated at a ground facility and then pumped into the aircraft's Liquid Nitrogen (LN_2) storage tanks during ground servicing and this Nitrogen is distributed to the fuel tanks during aircraft operation. For the onboard generator method, an Air Separation Module strips the Oxygen molecules from a stream of atmospheric air (consisting of 78% Nitrogen and 21% Oxygen), sending the Oxygen overboard as waste and the remaining Nitrogen to the fuel tanks.

In this thesis paper the onboard storage method is identified as FTIS Architecture #1. It is the least complex but the heaviest solution. For FTIS Architecture #2 & #3, onboard Nitrogen generation is utilized with two very different methods of supplying the necessary atmospheric air. FTIS Architecture #2 is connected to the aircraft's engines for a supply of hot air bled from a mid-stage port on each engine's casing, known as Bleed Air. Bleed Air is also utilized by the wing anti-ice system and the cabin environmental control system, among others. FTIS Architecture #3 is self-contained as it generates hot air with a FTIS-specific turbo compressor which is not shared with other aircraft systems. FTIS Architecture #2 provides the aircraft with the least weight penalty but is the most complex. FTIS Architecture #3 resides in a weight and complexity position between the other two architectures. A SysML Specialization diagram shows the three types of FTIS in Figure 5.

Comparisons and evaluations of the three FTIS architectures includes Block Diagrams and Internal Block Diagrams utilizing SysML. To illustrate compliance with customer requirements, a Use Case Diagram is also included for each system architecture.

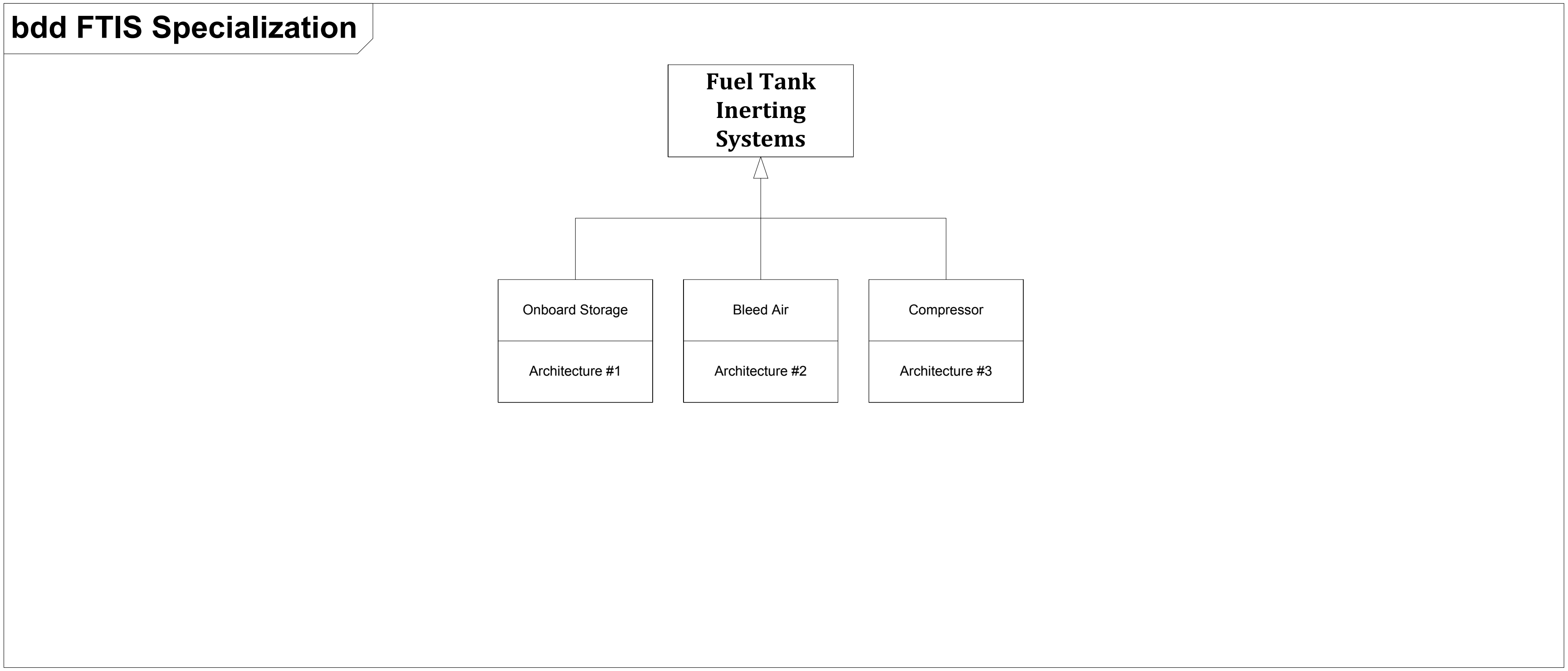


Figure 5: The Three FTIS Architectures

REQUIREMENTS DEVELOPMENT

The constraints, also known as controls per INCOSE (International Council On Systems Engineering), in the architecture design process for an FTIS are predominately related to the Federal Aviation Administration as FARs or Federal Aviation Regulations. Supporting the FARs are the two documents from the RTCA, DO-178B and DO-254, which describe the processes for developing airborne software and complex electronic hardware. Also, from the Society of Automotive Engineers (SAE) is a document regulating the process for developing airborne systems, the SAE Aerospace Recommended Practice, Guidelines for Development of Civil Aircraft and Systems, ARP-4754A.

The three competing FTIS architectures for this thesis paper will be developed per customer requirements from the Bombardier Aerospace (BA) company which builds air transport, regional, commuter and business aircraft. BA provides enablers to the architecture design process such well-defined electrical, mechanical and pneumatic interface characteristics, plus the physical environment and user interface requirements. The following customer requirements are intended for a new aircraft development program referred to as the BA-500.

Bombardier Aerospace Requirements

BA-500-01: The FTIS shall ensure that the oxygen concentration in the fuel tank ullage is always below that required for certification.

BA-500-02: The FTIS Supplier shall minimize and define the envelope into which the FTIS shall be installed.

BA-500-03: The FTIS shall not present an undue load to the air generation subsystem.

BA-500-04: The FTIS shall be capable of providing NEA during any aircraft operating phase.

BA-500-05: The FTIS shall be designed to provide a compact system to fit within an area between the fuel tank and the aircraft Belly Fairing.

BA-500-06: The FTIS shall not expose the aircraft to any catastrophic failure modes not demonstrated to have a probability of 10^{-9} or less.

BA-500-07: The FTIS system Guaranteed Not to Exceed Weight (GNTEW) shall not exceed 75 lbs dry weight (structures mounting bracketry not included).

BA-500-08: The FTIS system is to be sized to satisfy a minimum performance growth provision of 15%.

BA-500-09: Vibration levels introduced by the FTIS into the Aircraft structure shall be kept as low as practical in order to limit structural vibration and/or cabin noise.

BA-500-10: The NEA delivered by the FTIS shall not contain self-generated contaminants greater than those specified in FAR25.831, ‘Ventilation’.

BA-500-11: The FTIS waste exhaust shall be designed to safely discharge O_2 enriched air, water drainage or heat exchanger air in a manner safe for personnel working around or servicing the aircraft.

BA-500-12: The FTIS shall be controlled by solid-state devices.

BA-500-13: The FTIS shall be capable of unattended operation.

BA-500-14: The FTIS shall provide NEA to maintain the fuel tank in a non-flammable (inert) condition throughout all normal flight and ground conditions.

BA-500-15: The FTIS system shall provide nitrogen enriched air (NEA) to maintain a non-flammable mixture of air and fuel vapors in the fuels tank, in accordance with certification regulations

System Requirements

The development of system architecture and the allocation of customer high-level requirements to system requirements is governed by Section 4.4 of ARP4754A[12]: “The system architecture establishes the structure and boundaries within which specific item designs are implemented to meet the established requirements. More than one candidate system architecture may be considered for implementation." The SAE document continues to describe the importance of fully and accurately developing system requirements from the allocated customer requirements: “The decomposition and allocation of requirements to items should also ensure that the item can be shown to fully implement the allocated requirements. The process is complete when all requirements can be accommodated within the final architecture.” Table 1 shows the system-level requirements that have been decomposed from the customer’s high-level requirements along with their traceability to the high-level requirements.

Note: In this Systems Requirement Document, the FTIS will be identified as “the system”.

.

[12] SAE Aerospace ARP4754A: Guidelines for Development of Civil Aircraft and Systems

Table 1: System-level Requirements

Requirement Number	Requirement Description	Tracing and Notes
FTIS-001	The system shall employ a filtration device capable of reducing NEA contaminants to less than specified in FAR 25.831, if the FTIS originating source of NEA is atmospheric.	FAR 25.831 spec requires HEPA filter. Not necessary for onboard storage method (FTIS Arch. #1) Traces to: BA-500-10
FTIS -002	The system shall monitor the NEA percentage of oxygen during each flight, to ensure compliance with inerting certification levels.	Traces to: BA-500-01, BA-500-15
FTIS -003	The combined weight of all FTIS components shall not exceed 75 lbs.	Traces to: BA-500-07
FTIS -004	The system shall not include any flight deck controls, including an on/off switch.	Traces to: BA-500-13, BA-500-01 Allowing crew control could jeopardize constant inerting.
FTIS -005	Power for all electrical FTIS components, valve on/off and flow control shall be provided by a microprocessor or microcontroller working in conjunction with solid-state devices.	Traces to: BA-500-12 Solid-state devices are necessary for handling the valve solenoid currents.
FTIS -006	The FTIS shall not contain electromechanical devices such as micro switches or relays.	Traces to: BA-500-12 Bombardier's concern is with system reliability so Hall-effect sensors may be necessary for detecting valve position.
FTIS -007	The FTIS development team shall minimize system volume by utilizing CATIA in a shared Bombardier database.	Traces to: BA-500-02, BA-500-05

Requirement Number	Requirement Description	Tracing and Notes
FTIS -008	All FTIS valve mounts shall contain dampening material to minimize transmitted vibrations.	Traces to: BA-500-09
FTIS -009	If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS shall include a heat exchanger and cooling fan supplemented with ram air.	Traces to: BA-500-14, BA-500-04
FTIS -010	If the system architecture includes OEA and /or heat exchanger exhaust, both shall be combined in an outlet port located in a low-pressure zone just aft of the belly fairing.	Traces to: BA-500-11 Both OEA and HX exhaust are capable of injuring ground personnel.
FTIS -011	If the system architecture includes utilizing bleed air from the aircraft's main engines, the FTIS shall be capable of temporary shutdown during in-flight restarts with wing anti-ice activated.	Traces to: BA-500-03
FTIS -012	If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS shall include temperature sensing and control sufficient for exceeding reliability of 10-9.	Traces to: BA-500-06 Combined reliability of temperature sensors, A/D converters, microprocessor and control circuit provides just 10-7 reliability. Two completely independent sensing/control blocks are needed.
FTIS -013	All FTIS components shall be designed to provide 15% inerting margin.	Traces to: BA-500-08
FTIS -014	The system shall communicate with aircraft systems such as the air data system for FTIS flow control.	Traces to: BA-500-04, BA-500-13

Requirement Number	Requirement Description	Tracing and Notes
FTIS -015	The system *shall* communicate with aircraft systems such as the air supply system and landing gear system for FTIS mode control.	Traces to: BA-500-03, BA-500-13 Not necessary for onboard storage method (FTIS Arch. #1).

Requirements Trace Matrix

Table 2 provides a concise traceability matrix between the customer requirements and their allocation to system requirements.

Table 2: Customer to System Requirement Tracing

Customer Requirement	System Requirement(s)
BA-500-01	FTIS-002, FTIS -004
BA-500-02	FTIS-007
BA-500-03	FTIS-011, FTIS-015
BA-500-04	FTIS-009, FTIS-014
BA-500-05	FTIS-007
BA-500-06	FTIS-012
BA-500-07	FTIS-003
BA-500-08	FTIS-013
BA-500-09	FTIS-008
BA-500-10	FTIS-001
BA-500-11	FTIS-010
BA-500-12	FTIS-005, FTIS-006
BA-500-13	FTIS-004, FTIS-014, FTIS-015
BA-500-14	FTIS-009
BA-500-15	FTIS-002

Requirements Discussion

This section of this Thesis paper shall attempt to explain the reasoning behind the flowdown (decomposition) from customer requirements to system requirements. This discussion is commonly expected by auditors of the system certification process, typically at the aircraft manufacturer (customer) level but can also be examined by the certification authorities.

An important characteristic of the customer requirements is none of them direct the system supplier to a particular system architecture nor an implementation of a specific technology. Just one customer requirement approaches a directive to an architecture or a technology: BA-500-11: The FTIS waste exhaust shall be designed to safely discharge O2 enriched air, water drainage or heat exchanger air in a manner safe for personnel working around or servicing the aircraft. This requirement was written with the assumption that if the system supplier utilizes a system architecture which does not include FTIS waste exhaust in the form of any of the three listed in the requirement, then the requirement doesn’t need to be complied with because it doesn’t apply to the selected system architecture.

A fundamental step in developing system requirements from customer requirements, known as decomposing or flowing-down the requirements (as per ARP-4754A), is identifying stakeholders. A stakeholder is any entity or person having a vested interest in the system being developed which can range from the end-user to the company sponsoring the project and on to the certifying authorities. For this Thesis paper, the identified stakeholders are: the certifying authority, in this case Transport Canada; the customer, Bombardier; the end-users, identified in the Use Case diagrams as aircraft owner/operator; and last but not least, the FTIS manufacturer.

Customer-level requirements may be driven by many constraints and priorities such as physical limits, FARs, lessons learned, safety considerations and business goals. The system-level requirements these customer-level requirements are decomposed into must focus on stakeholders. To the system engineer, meeting a safety-driven requirement is just as important as complying with a functional requirement, even though from a system certification standpoint the safety considerations carry the most criticality and cannot be ignored. When choosing between various system architectures, one system-level requirement should not be weighted more or less than any other; all system-level requirements carry the same importance.

More important than competing to meet as many system-level requirements as possible is the necessity to meet all customer-level requirements, if this is possible for any system architecture. Utilizing use case diagrams to determine the optimal system architecture is on the critical path to resolving this thesis' problem statement.

A summary comparison of the three architectures' requirement coverage is given in the CONCLUSIONS section of this thesis paper.

USE CASE DIAGRAMS

The following use case diagrams will graphically demonstrate the requirement "holes" in each system architecture by modeling the respective system's context. In each use case diagram all system requirements are displayed with a link to every stakeholder. If a requirement is shown without a corresponding link, that requirement is not met by that system architecture. A table containing a tally of the customer-level requirements met by each architecture and then a sum of requirements met will be used to rank each architecture.

In section 7.5.3.4 of SysML for Systems Engineering[13], authors Jon Holt and Simon Perry assert that a requirement, represented by a use case, which has no connection to an Actor can only be explained by four reasons, as shown in Figure 6:

[13] SysML for Systems Engineering © 2008 The Institution of Engineering and Technology

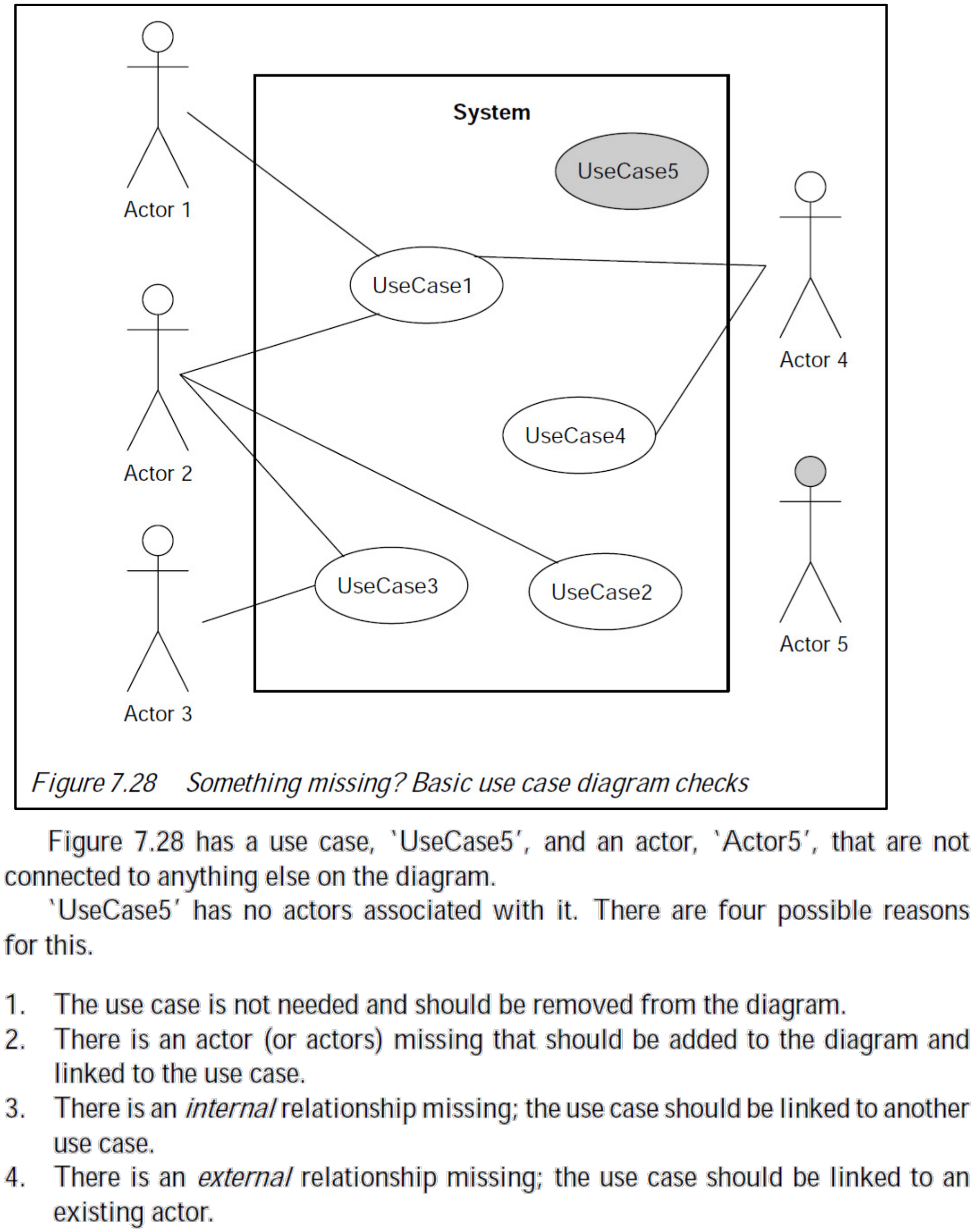

System
UseCase5
Actor 1
UseCase1
Actor 4
Actor 2
UseCase4
Actor 3
UseCase3
UseCase2
Actor 5

Figure 7.28 Something missing? Basic use case diagram checks

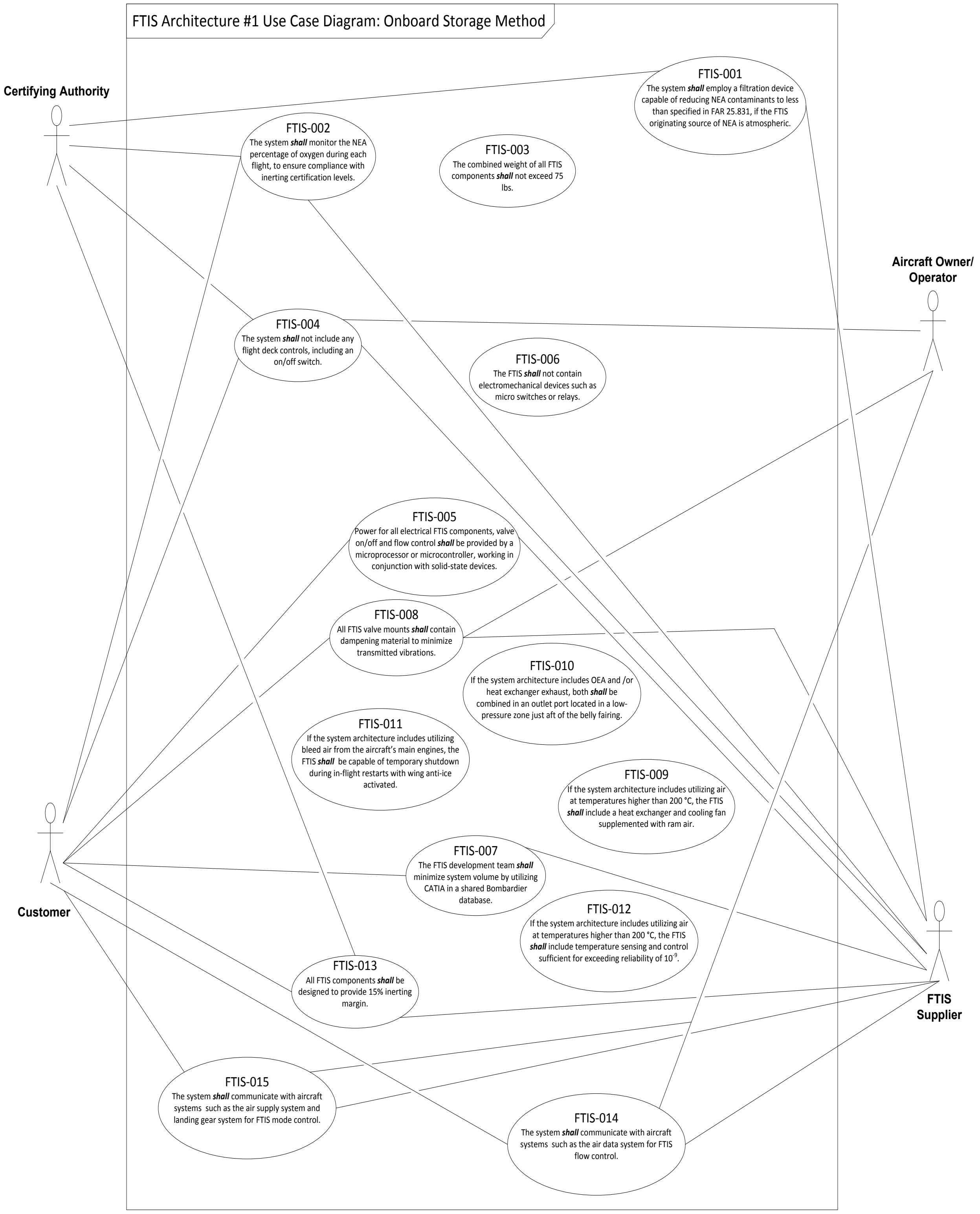
Figure 7.28 has a use case, 'UseCase5', and an actor, 'Actor5', that are not connected to anything else on the diagram.

'UseCase5' has no actors associated with it. There are four possible reasons for this.

1. The use case is not needed and should be removed from the diagram.
2. There is an actor (or actors) missing that should be added to the diagram and linked to the use case.
3. There is an *internal* relationship missing; the use case should be linked to another use case.
4. There is an *external* relationship missing; the use case should be linked to an existing actor.

Figure 6: Use Case to Actor Relationship, per Holt & Perry

This thesis paper will add a fifth reason, which is: the requirement is not covered by the chosen system architecture.



FTIS-001
The system *shall* employ a filtration device capable of reducing NEA contaminants to less than specified in FAR 25.831, if the FTIS originating source of NEA is atmospheric.

FTIS-002
The system *shall* monitor the NEA percentage of oxygen during each flight, to ensure compliance with inerting certification levels.

FTIS-003
The combined weight of all FTIS components *shall* not exceed 75 lbs.

FTIS-004
The system *shall* not include any flight deck controls, including an on/off switch.

FTIS-006
The FTIS *shall* not contain electromechanical devices such as micro switches or relays.

FTIS-005
Power for all electrical FTIS components, valve on/off and flow control *shall* be provided by a microprocessor or microcontroller, working in conjunction with solid-state devices.

FTIS-008
All FTIS valve mounts *shall* contain dampening material to minimize transmitted vibrations.

FTIS-010
If the system architecture includes OEA and /or heat exchanger exhaust, both *shall* be combined in an outlet port located in a low-pressure zone just aft of the belly fairing.

FTIS-011
If the system architecture includes utilizing bleed air from the aircraft's main engines, the FTIS *shall* be capable of temporary shutdown during in-flight restarts with wing anti-ice activated.

FTIS-009
If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS *shall* include a heat exchanger and cooling fan supplemented with ram air.

FTIS-007
The FTIS development team *shall* minimize system volume by utilizing CATIA in a shared Bombardier database.

FTIS-012
If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS *shall* include temperature sensing and control sufficient for exceeding reliability of 10^{-9}.

FTIS-013
All FTIS components *shall* be designed to provide 15% inerting margin.

FTIS-015
The system *shall* communicate with aircraft systems such as the air supply system and landing gear system for FTIS mode control.

FTIS-014
The system *shall* communicate with aircraft systems such as the air data system for FTIS flow control.

Figure 7: FTIS Architecture #1 Use Case Diagram: Onboard Storage

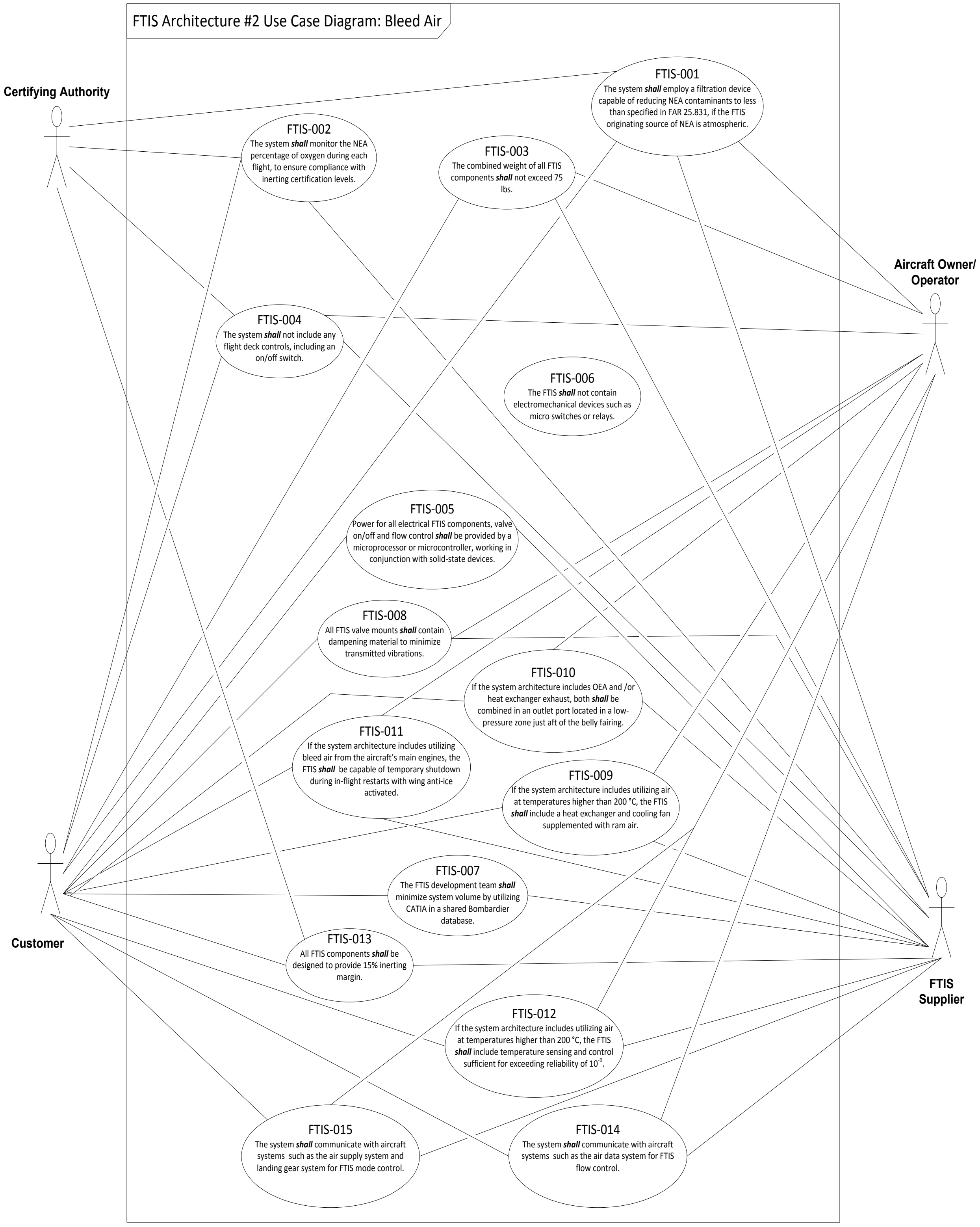

FTIS Architecture #2 Use Case Diagram: Bleed Air
Certifying Authority
FTIS-001
The system *shall* employ a filtration device capable of reducing NEA contaminants to less than specified in FAR 25.831, if the FTIS originating source of NEA is atmospheric.
FTIS-002
The system *shall* monitor the NEA percentage of oxygen during each flight, to ensure compliance with inerting certification levels.
FTIS-003
The combined weight of all FTIS components *shall* not exceed 75 lbs.
Aircraft Owner/ Operator
FTIS-004
The system *shall* not include any flight deck controls, including an on/off switch.
FTIS-006
The FTIS *shall* not contain electromechanical devices such as micro switches or relays.
FTIS-005
Power for all electrical FTIS components, valve on/off and flow control *shall* be provided by a microprocessor or microcontroller, working in conjunction with solid-state devices.
FTIS-008
All FTIS valve mounts *shall* contain dampening material to minimize transmitted vibrations.
FTIS-010
If the system architecture includes OEA and /or heat exchanger exhaust, both *shall* be combined in an outlet port located in a low-pressure zone just aft of the belly fairing.
FTIS-011
If the system architecture includes utilizing bleed air from the aircraft's main engines, the FTIS *shall* be capable of temporary shutdown during in-flight restarts with wing anti-ice activated.
FTIS-009
If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS *shall* include a heat exchanger and cooling fan supplemented with ram air.
FTIS-007
The FTIS development team *shall* minimize system volume by utilizing CATIA in a shared Bombardier database.
Customer
FTIS-013
All FTIS components *shall* be designed to provide 15% inerting margin.
FTIS Supplier
FTIS-012
If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS *shall* include temperature sensing and control sufficient for exceeding reliability of 10^{-9}.
FTIS-015
The system *shall* communicate with aircraft systems such as the air supply system and landing gear system for FTIS mode control.
FTIS-014
The system *shall* communicate with aircraft systems such as the air data system for FTIS flow control.

Figure 8: FTIS Architecture #2 Use Case Diagram: Bleed Air

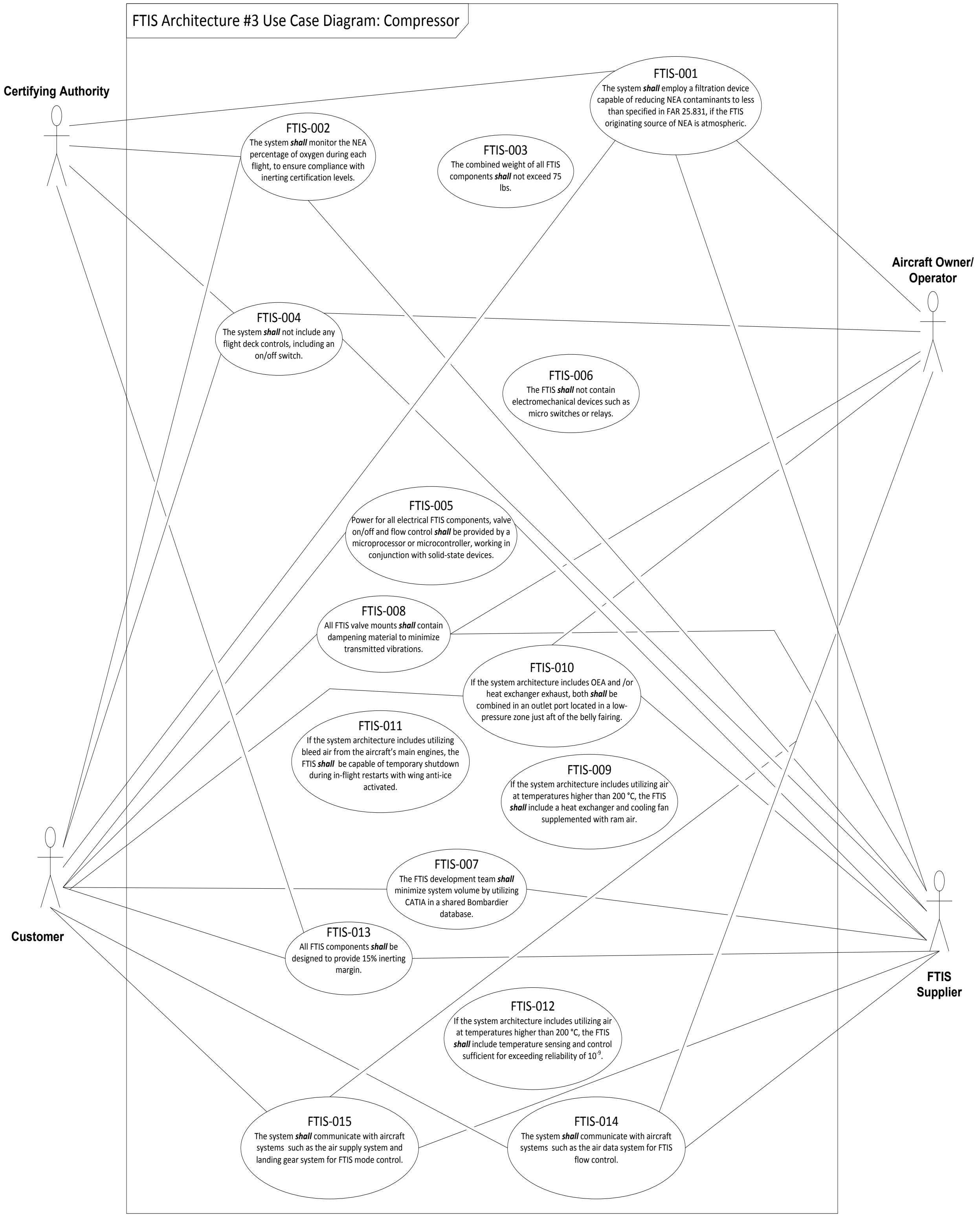

FTIS Architecture #3 Use Case Diagram: Compressor
Certifying Authority
Aircraft Owner/ Operator
Customer
FTIS Supplier
FTIS-001
The system shall employ a filtration device capable of reducing NEA contaminants to less than specified in FAR 25.831, if the FTIS originating source of NEA is atmospheric.
FTIS-002
The system shall monitor the NEA percentage of oxygen during each flight, to ensure compliance with inerting certification levels.
FTIS-003
The combined weight of all FTIS components shall not exceed 75 lbs.
FTIS-004
The system shall not include any flight deck controls, including an on/off switch.
FTIS-006
The FTIS shall not contain electromechanical devices such as micro switches or relays.
FTIS-005
Power for all electrical FTIS components, valve on/off and flow control shall be provided by a microprocessor or microcontroller, working in conjunction with solid-state devices.
FTIS-008
All FTIS valve mounts shall contain dampening material to minimize transmitted vibrations.
FTIS-010
If the system architecture includes OEA and /or heat exchanger exhaust, both shall be combined in an outlet port located in a low-pressure zone just aft of the belly fairing.
FTIS-011
If the system architecture includes utilizing bleed air from the aircraft's main engines, the FTIS shall be capable of temporary shutdown during in-flight restarts with wing anti-ice activated.
FTIS-009
If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS shall include a heat exchanger and cooling fan supplemented with ram air.
FTIS-007
The FTIS development team shall minimize system volume by utilizing CATIA in a shared Bombardier database.
FTIS-013
All FTIS components shall be designed to provide 15% inerting margin.
FTIS-012
If the system architecture includes utilizing air at temperatures higher than 200 °C, the FTIS shall include temperature sensing and control sufficient for exceeding reliability of 10^{-9}.
FTIS-015
The system shall communicate with aircraft systems such as the air supply system and landing gear system for FTIS mode control.
FTIS-014
The system shall communicate with aircraft systems such as the air data system for FTIS flow control.

Figure 9: FTIS Architecture #3 Use Case Diagram: Compressor

Use Case Summary

So, of what use are use case diagrams? For this study of competing FTIS architectures, the use case diagram provides a quickly recognizable graphic of which system architecture complies with the most system requirements. But complying with system requirements are only part of the requirements analysis, as complying with all the customer-level requirements is the true goal of supplying a system to the customer.

The use case diagrams in this thesis paper show the links to system-level requirements because those are the requirements to which each system architecture is designed. With each customer-level requirement possibly covered by multiple system-level requirements, each FTIS architecture has more than one graphical opportunity to display compliance with a particular customer-level requirement.

In the following Requirements Summary tables, a customer requirement is considered to be complied with only if all system-level requirements that trace to it are either met or not applicable.

Table 3: FTIS Architecture #1: Onboard Storage – Requirements Summary

Customer-Level Requirement Complied With	System-Level Requirement Met	Customer-Level Requirement Not Complied With	System-Level Requirement Not Met
BA-500-01	FTIS-002 FTIS-004		
BA-500-02	FTIS-007		
BA-500-03	FTIS-015	Not Applicable – this architecture does not connect to the air generation subsystem	FTIS-011
BA-500-04	FTIS-014	Not Applicable – 200°C air not utilized by this architecture	FTIS-009

Customer-Level Requirement Complied With	System-Level Requirement Met	Customer-Level Requirement Not Complied With	System-Level Requirement Not Met
BA-500-05	FTIS-007		
BA-500-06		Not Applicable – this architecture avoids all Catastrophic failure modes	FTIS-012
		BA-500-07	FTIS-003
BA-500-08	FTIS-013		
BA-500-09	FTIS-008		
BA-500-10	FTIS-001		
BA-500-11		Not Applicable – this architecture does not produce waste exhaust	FTIS-010
	FTIS-005	BA-500-12	FTIS-006
BA-500-13	FTIS-004 FTIS-014 FTIS-015		
BA-500-14	FTIS-009		
BA-500-15	FTIS-002		

Customer requirements fully complied with 9

Customer requirements not applicable 4

Customer requirements not complied with 2

Table 4: FTIS Architecture #2: Bleed Air – Requirements Summary

Customer-Level Requirement Complied With	System-Level Requirement Met	Customer-Level Requirement Not Complied With	System-Level Requirement Not Met
BA-500-01	FTIS-002 FTIS-004		
BA-500-02	FTIS-007		
BA-500-03	FTIS-011 FTIS-015		
BA-500-04	FTIS-009 FTIS-014		
BA-500-05	FTIS-007		
BA-500-06	FTIS-012		
BA-500-07	FTIS-003		
BA-500-08	FTIS-013		
BA-500-09	FTIS-008		
BA-500-10	FTIS-001		
BA-500-11	FTIS-010		
	FTIS-005	BA-500-12	FTIS-006
BA-500-13	FTIS-004 FTIS-014 FTIS-015		
BA-500-14	FTIS-009		
BA-500-15	FTIS-002		

Customer requirements fully complied with 14

Customer requirements not applicable 0

Customer requirements not complied with 1

Table 5: FTIS Architecture #3: Compressor – Requirements Summary

Customer-Level Requirement Complied With	System-Level Requirement Met	Customer-Level Requirement Not Complied With	System-Level Requirement Not Met
BA-500-01	FTIS-002 FTIS-004		
BA-500-02	FTIS-007		
BA-500-03	FTIS-015	Not Applicable – this architecture does not connect to the air generation subsystem	FTIS-011
BA-500-04	FTIS-014	Not Applicable – 200°C air not utilized by this architecture	FTIS-009
BA-500-05	FTIS-007		
BA-500-06		Not Applicable – this architecture avoids all Catastrophic failure modes	FTIS-012
		BA-500-07	FTIS-003
BA-500-08	FTIS-013		
BA-500-09	FTIS-008		
BA-500-10	FTIS-001		
BA-500-11	FTIS-010		
	FTIS-005	BA-500-12	FTIS-006
BA-500-13	FTIS-004 FTIS-014 FTIS-015		
BA-500-14	FTIS-009		
BA-500-15	FTIS-002		

Customer requirements fully complied with 13

Customer requirements not applicable 0

Customer requirements not complied with 2

BLOCK DEFINITION DIAGRAMS

A Block Definition Diagram (BDD) for each FTIS architecture is included in Figure 10, Figure 11, and Figure 12 to model the structural aspects of each type of system.

Per the authoritative SysML for Systems Engineering, page 91: “Block definition diagrams realize a structural aspect of the model of a system and show what conceptual ‘things’ exist in a system and what relationships exist between them”. BDDs are used in this paper because they are the quickest method of portraying the varying levels of complexity between FTIS types. Comparing the BDD of FTIS Architecture #1, Onboard Storage, with the other two types that use an ASM, the lower complexity of FTIS Architecture #1 is immediately apparent.

An Internal Block Diagram (IBD) of each FTIS Architecture’s electronic controller is used to illustrate the large difference in structural complexity between controllers that would be used in each of the FTIS types. For the IBDs, which show the parts utilized within the Controlling block, the contrast between system types is not as striking, although a closer look at the IBDs reveals the Controlling element of Architecture #2 contains the most complexity.

The BDDs and IBDs for this thesis paper were created by the author using Microsoft Visio 2010 and a shapes stencil (a .vss file) obtained from the Object Modeling Group’s website: www.omgsysml.org.

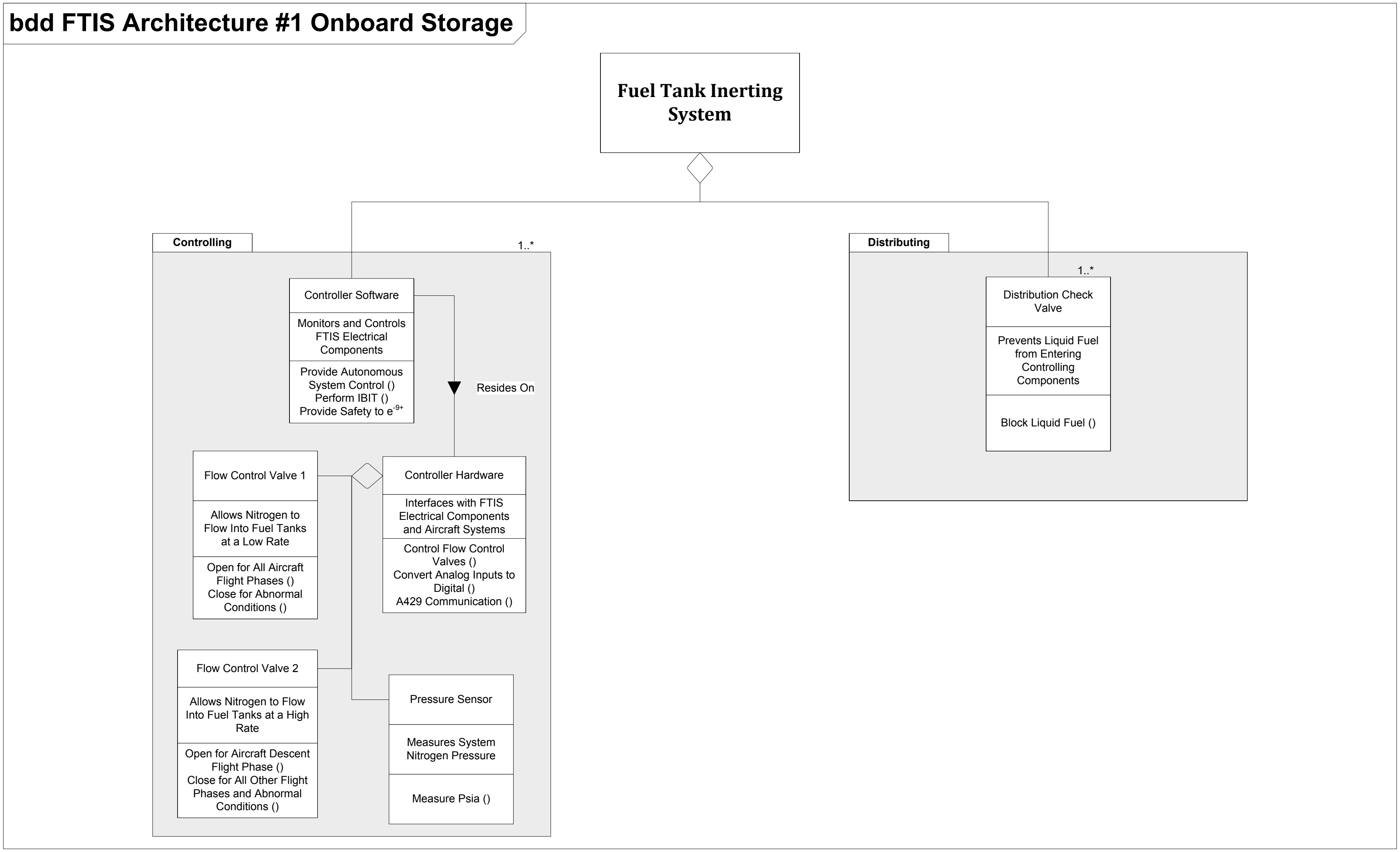

bdd FTIS Architecture #1 Onboard Storage
Fuel Tank Inerting System
Controlling
1..*
Controller Software
Monitors and Controls FTIS Electrical Components
Provide Autonomous System Control ()
Perform IBIT ()
Provide Safety to e-9+
Resides On
Flow Control Valve 1
Allows Nitrogen to Flow Into Fuel Tanks at a Low Rate
Open for All Aircraft Flight Phases ()
Close for Abnormal Conditions ()
Controller Hardware
Interfaces with FTIS Electrical Components and Aircraft Systems
Control Flow Control Valves ()
Convert Analog Inputs to Digital ()
A429 Communication ()
Flow Control Valve 2
Allows Nitrogen to Flow Into Fuel Tanks at a High Rate
Open for Aircraft Descent Flight Phase ()
Close for All Other Flight Phases and Abnormal Conditions ()
Pressure Sensor
Measures System Nitrogen Pressure
Measure Psia ()
Distributing
1..*
Distribution Check Valve
Prevents Liquid Fuel from Entering Controlling Components
Block Liquid Fuel ()

Figure 10: FTIS Architecture #1 Block Diagram: Onboard Storage

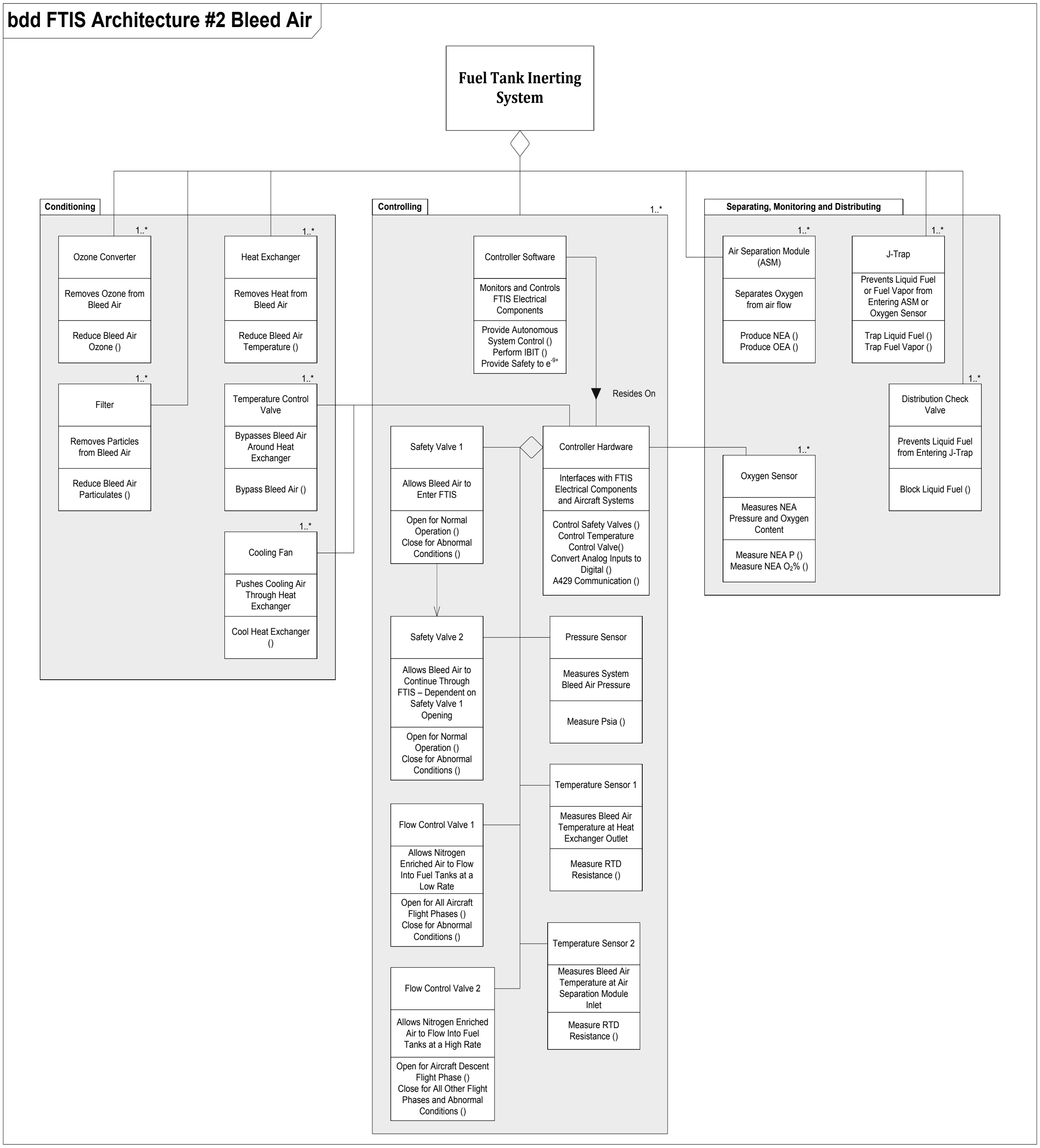

bdd FTIS Architecture #2 Bleed Air
Fuel Tank Inerting System
Conditioning
Controlling
1..*
Separating, Monitoring and Distributing
1..*
Ozone Converter
Removes Ozone from Bleed Air
Reduce Bleed Air Ozone ()
1..*
Heat Exchanger
Removes Heat from Bleed Air
Reduce Bleed Air Temperature ()
1..*
Filter
Removes Particles from Bleed Air
Reduce Bleed Air Particulates ()
1..*
Temperature Control Valve
Bypasses Bleed Air Around Heat Exchanger
Bypass Bleed Air ()
1..*
Cooling Fan
Pushes Cooling Air Through Heat Exchanger
Cool Heat Exchanger ()
Controller Software
Monitors and Controls FTIS Electrical Components
Provide Autonomous System Control ()
Perform IBIT ()
Provide Safety to e-9+
Resides On
Controller Hardware
Interfaces with FTIS Electrical Components and Aircraft Systems
Control Safety Valves ()
Control Temperature Control Valve()
Convert Analog Inputs to Digital ()
A429 Communication ()
Safety Valve 1
Allows Bleed Air to Enter FTIS
Open for Normal Operation ()
Close for Abnormal Conditions ()
Safety Valve 2
Allows Bleed Air to Continue Through FTIS – Dependent on Safety Valve 1 Opening
Open for Normal Operation ()
Close for Abnormal Conditions ()
Pressure Sensor
Measures System Bleed Air Pressure
Measure Psia ()
Temperature Sensor 1
Measures Bleed Air Temperature at Heat Exchanger Outlet
Measure RTD Resistance ()
Flow Control Valve 1
Allows Nitrogen Enriched Air to Flow Into Fuel Tanks at a Low Rate
Open for All Aircraft Flight Phases ()
Close for Abnormal Conditions ()
Temperature Sensor 2
Measures Bleed Air Temperature at Air Separation Module Inlet
Measure RTD Resistance ()
Flow Control Valve 2
Allows Nitrogen Enriched Air to Flow Into Fuel Tanks at a High Rate
Open for Aircraft Descent Flight Phase ()
Close for All Other Flight Phases and Abnormal Conditions ()
1..*
Air Separation Module (ASM)
Separates Oxygen from air flow
Produce NEA ()
Produce OEA ()
1..*
J-Trap
Prevents Liquid Fuel or Fuel Vapor from Entering ASM or Oxygen Sensor
Trap Liquid Fuel ()
Trap Fuel Vapor ()
1..*
Distribution Check Valve
Prevents Liquid Fuel from Entering J-Trap
Block Liquid Fuel ()
1..*
Oxygen Sensor
Measures NEA Pressure and Oxygen Content
Measure NEA P ()
Measure NEA O2% ()

Figure 11: FTIS Architecture #2 Block Diagram: Bleed Air

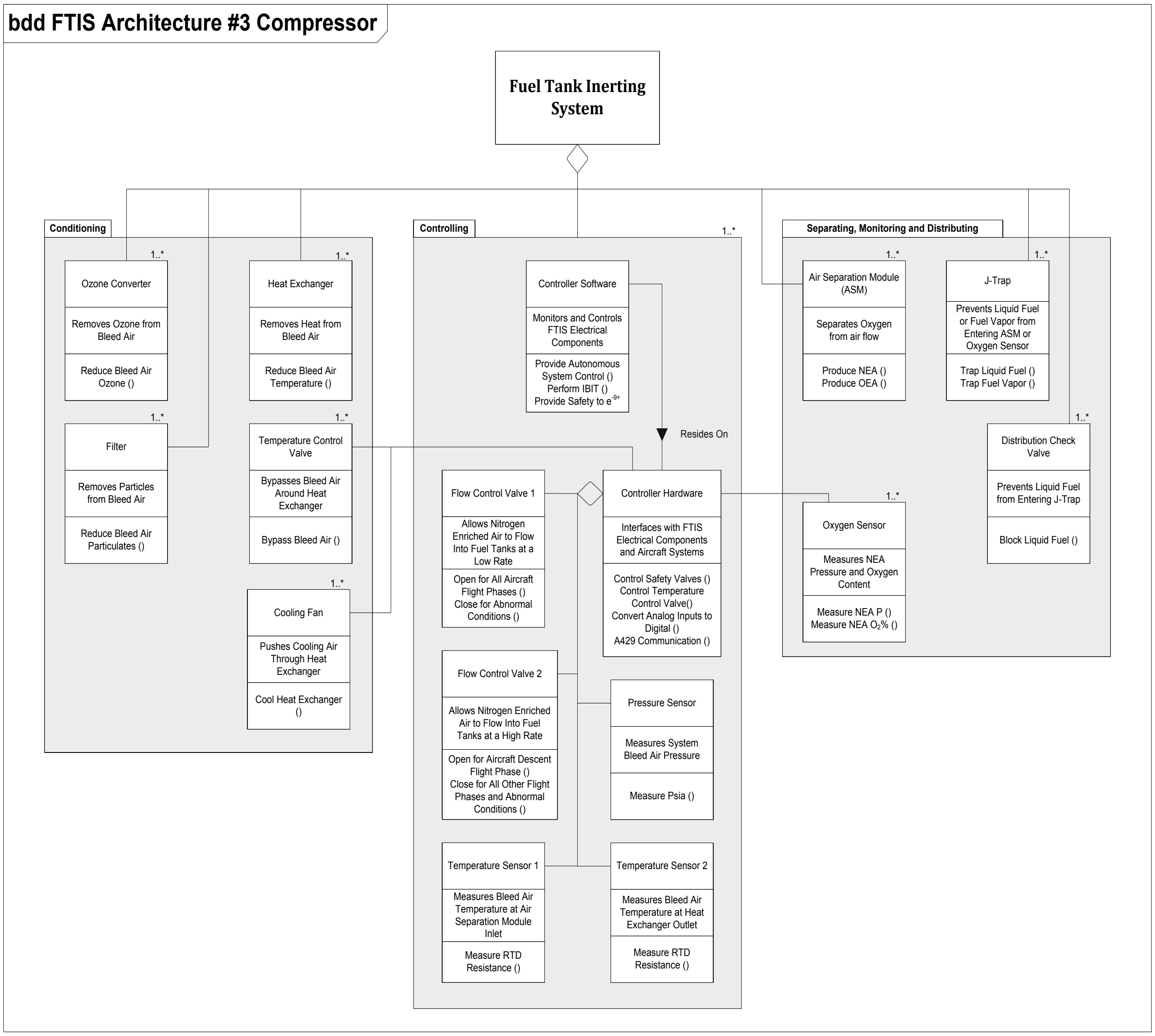

bdd FTIS Architecture #3 Compressor
Fuel Tank Inerting System
Conditioning
1..*
Ozone Converter
Removes Ozone from Bleed Air
Reduce Bleed Air Ozone ()
1..*
Heat Exchanger
Removes Heat from Bleed Air
Reduce Bleed Air Temperature ()
1..*
Filter
Removes Particles from Bleed Air
Reduce Bleed Air Particulates ()
1..*
Temperature Control Valve
Bypasses Bleed Air Around Heat Exchanger
Bypass Bleed Air ()
1..*
Cooling Fan
Pushes Cooling Air Through Heat Exchanger
Cool Heat Exchanger ()
Controlling
1..*
Controller Software
Monitors and Controls FTIS Electrical Components
Provide Autonomous System Control ()
Perform IBIT ()
Provide Safety to e-9+
Resides On
Flow Control Valve 1
Allows Nitrogen Enriched Air to Flow Into Fuel Tanks at a Low Rate
Open for All Aircraft Flight Phases ()
Close for Abnormal Conditions ()
Controller Hardware
Interfaces with FTIS Electrical Components and Aircraft Systems
Control Safety Valves ()
Control Temperature Control Valve()
Convert Analog Inputs to Digital ()
A429 Communication ()
Flow Control Valve 2
Allows Nitrogen Enriched Air to Flow Into Fuel Tanks at a High Rate
Open for Aircraft Descent Flight Phase ()
Close for All Other Flight Phases and Abnormal Conditions ()
Pressure Sensor
Measures System Bleed Air Pressure
Measure Psia ()
Temperature Sensor 1
Measures Bleed Air Temperature at Air Separation Module Inlet
Measure RTD Resistance ()
Temperature Sensor 2
Measures Bleed Air Temperature at Heat Exchanger Outlet
Measure RTD Resistance ()
Separating, Monitoring and Distributing
1..*
Air Separation Module (ASM)
Separates Oxygen from air flow
Produce NEA ()
Produce OEA ()
1..*
J-Trap
Prevents Liquid Fuel or Fuel Vapor from Entering ASM or Oxygen Sensor
Trap Liquid Fuel ()
Trap Fuel Vapor ()
1..*
Distribution Check Valve
Prevents Liquid Fuel from Entering J-Trap
Block Liquid Fuel ()
1..*
Oxygen Sensor
Measures NEA Pressure and Oxygen Content
Measure NEA P ()
Measure NEA O2% ()

Figure 12: FTIS Architecture #3 Block Diagram: Compressor

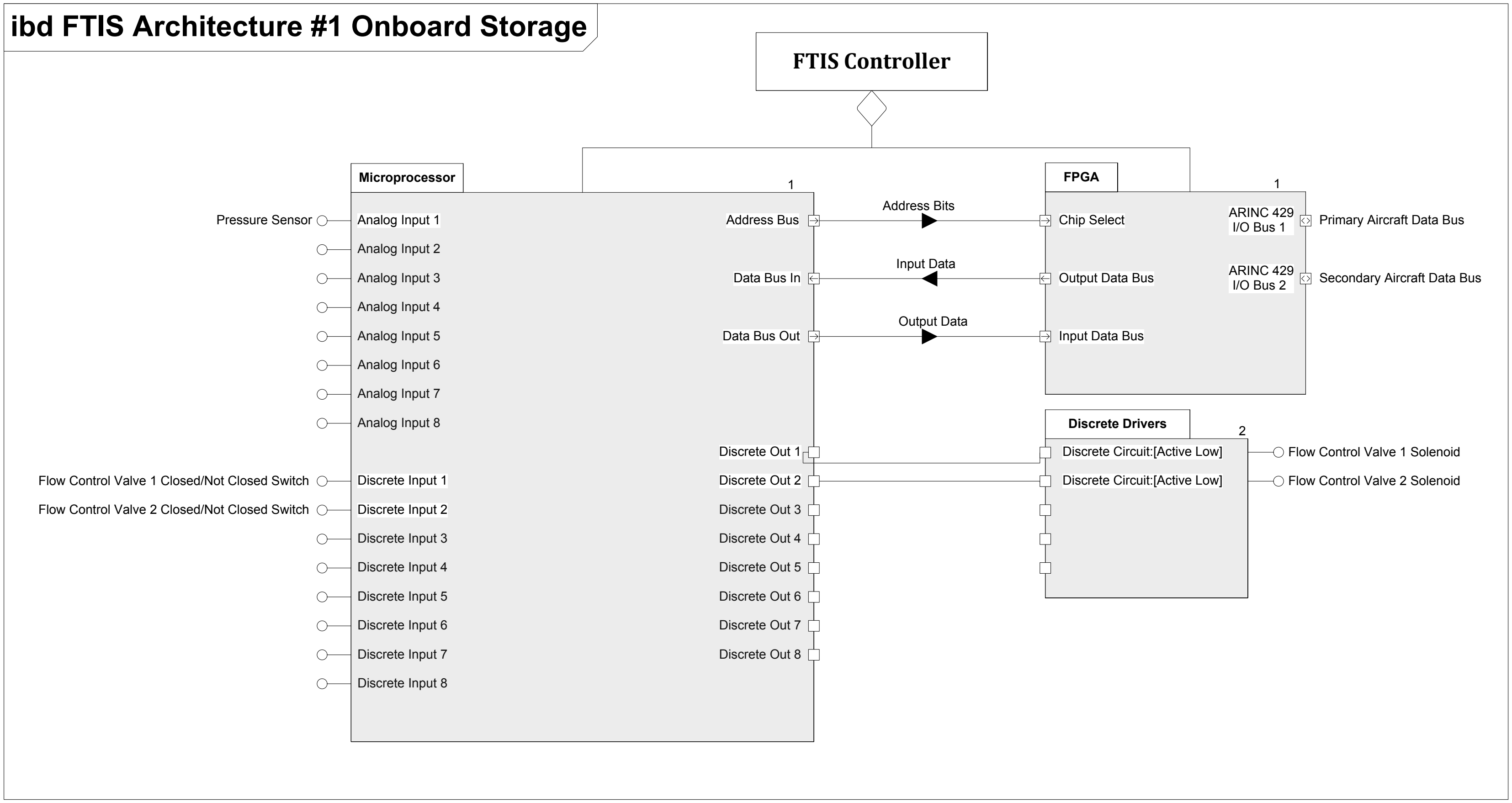


Figure 13: FTIS Architecture #1 Internal Block Diagram: Onboard Storage

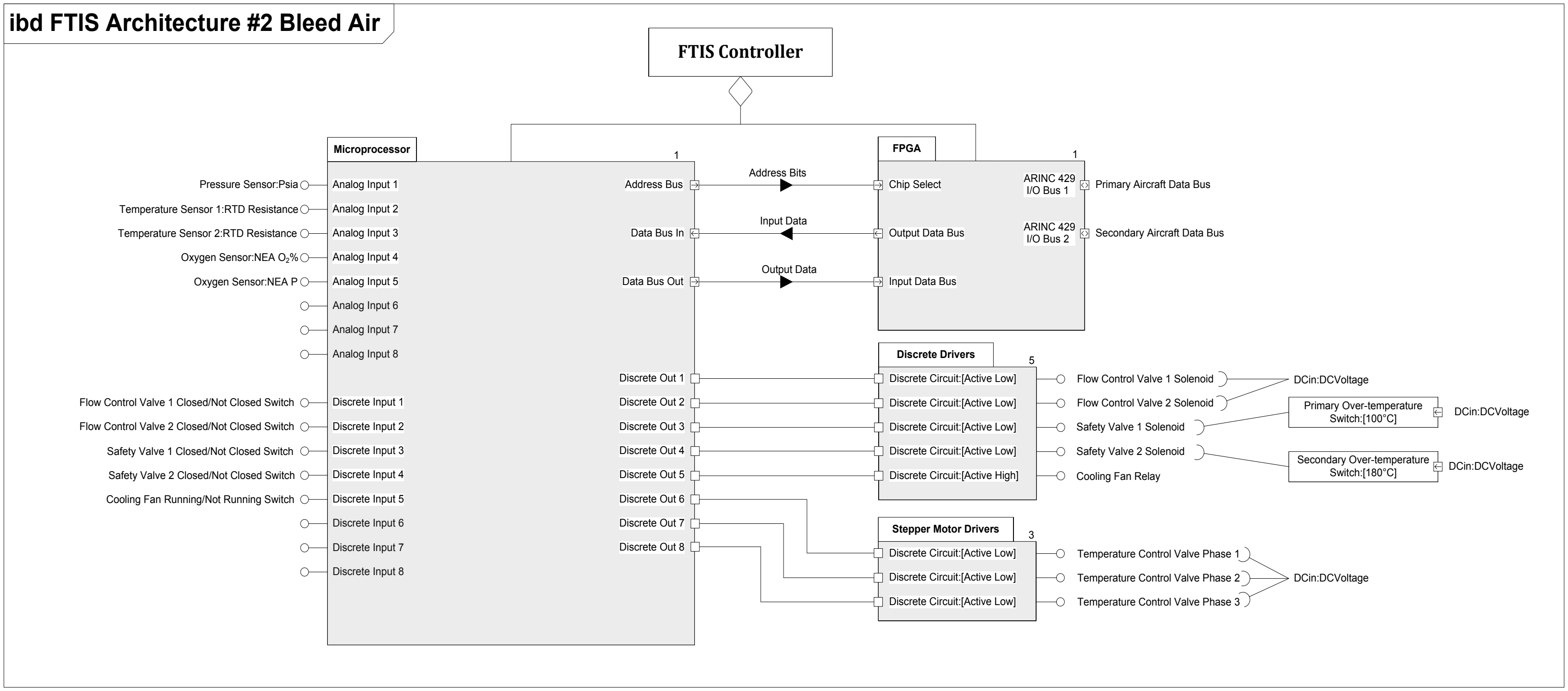

ibd FTIS Architecture #2 Bleed Air
FTIS Controller
Microprocessor
1
FPGA
1
Pressure Sensor:Psia
Temperature Sensor 1:RTD Resistance
Temperature Sensor 2:RTD Resistance
Oxygen Sensor:NEA O$_2$%
Oxygen Sensor:NEA P
Analog Input 1
Analog Input 2
Analog Input 3
Analog Input 4
Analog Input 5
Analog Input 6
Analog Input 7
Analog Input 8
Address Bus
Data Bus In
Data Bus Out
Address Bits
Input Data
Output Data
Chip Select
Output Data Bus
Input Data Bus
ARINC 429 I/O Bus 1
ARINC 429 I/O Bus 2
Primary Aircraft Data Bus
Secondary Aircraft Data Bus
Flow Control Valve 1 Closed/Not Closed Switch
Flow Control Valve 2 Closed/Not Closed Switch
Safety Valve 1 Closed/Not Closed Switch
Safety Valve 2 Closed/Not Closed Switch
Cooling Fan Running/Not Running Switch
Discrete Input 1
Discrete Input 2
Discrete Input 3
Discrete Input 4
Discrete Input 5
Discrete Input 6
Discrete Input 7
Discrete Input 8
Discrete Out 1
Discrete Out 2
Discrete Out 3
Discrete Out 4
Discrete Out 5
Discrete Out 6
Discrete Out 7
Discrete Out 8
Discrete Drivers
5
Discrete Circuit:[Active Low]
Discrete Circuit:[Active Low]
Discrete Circuit:[Active Low]
Discrete Circuit:[Active Low]
Discrete Circuit:[Active High]
Flow Control Valve 1 Solenoid
Flow Control Valve 2 Solenoid
Safety Valve 1 Solenoid
Safety Valve 2 Solenoid
Cooling Fan Relay
DCin:DCVoltage
Primary Over-temperature Switch:[100°C]
DCin:DCVoltage
Secondary Over-temperature Switch:[180°C]
DCin:DCVoltage
Stepper Motor Drivers
3
Discrete Circuit:[Active Low]
Discrete Circuit:[Active Low]
Discrete Circuit:[Active Low]
Temperature Control Valve Phase 1
Temperature Control Valve Phase 2
Temperature Control Valve Phase 3
DCin:DCVoltage

Figure 14: FTIS Architecture #2 Internal Block Diagram: Bleed Air

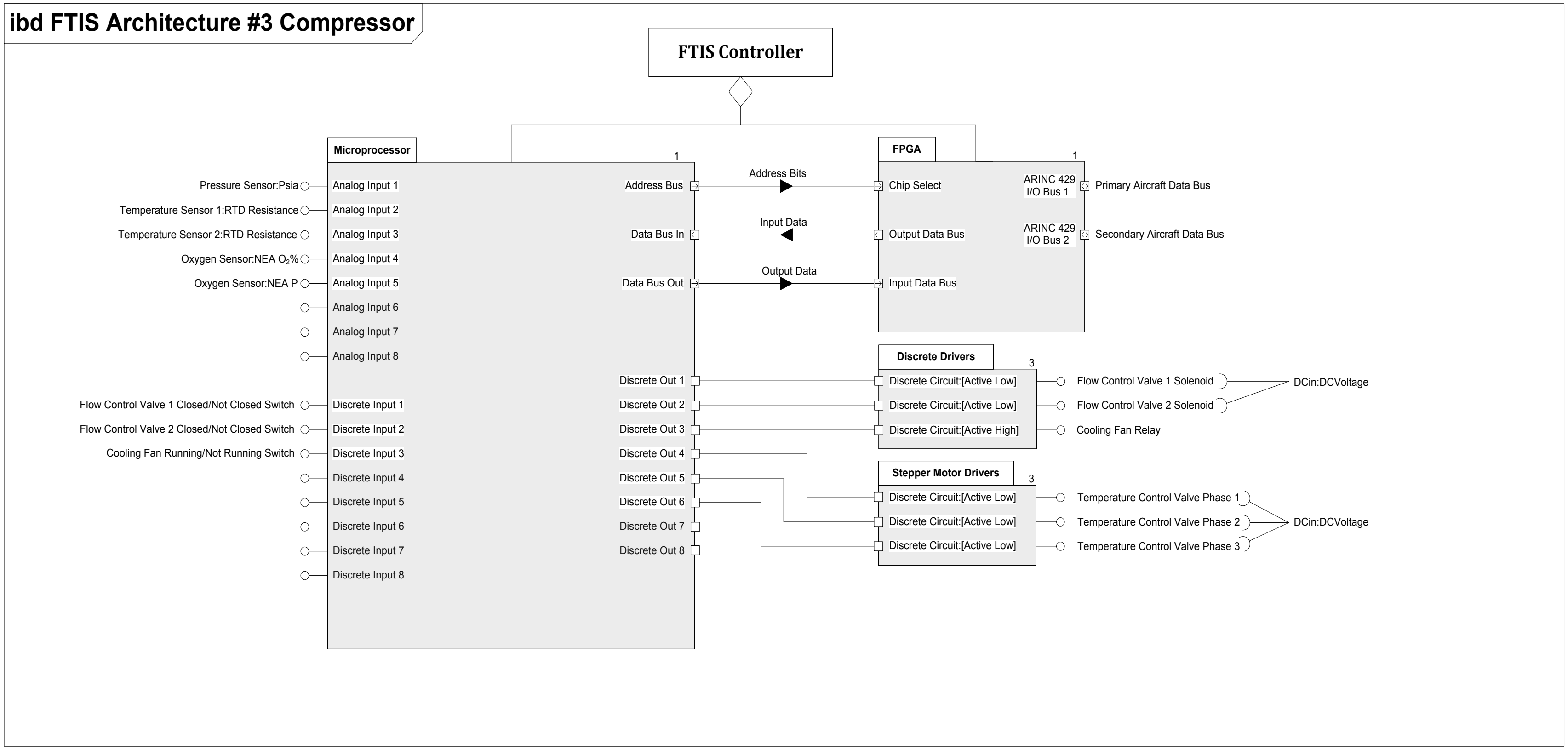


Figure 15: FTIS Architecture #3 Internal Block Diagram: Compressor

SYSTEM COMPLEXITY CONSIDERATIONS

Safety Requirements

System complexity is a large consideration in choosing an aircraft system architecture, for many reasons. The most obvious to the majority of readers of this paper is a lower system complexity means a lower parts count, which in turn means higher system reliability and lower supply chain costs. Better reliability and lower costs are great for any industry’s systems, but in aviation an airborne system must meet safety requirements before all others. For example, one of the first steps in designing a new aircraft is creating a System Functional Hazard Assessment (SFHA). This is done by the aircraft manufacturer with oversight from the certifying authorities. An example SHFA is shown in Table 6.

Table 6: System Functional Hazard Assessment for an FTIS

Function: Provide Temperature Limited Nitrogen Enriched Air to Fuel Tanks						
Type of Hazard	Flight Phase	Effect on Aircraft	Pilot Recognition Method	Pilot Action	Criticality	Safety Requirement
Unannunciated loss of sufficient nitrogen enriched air supply to the fuel tank	ALL	Reduction in oxygen displacement capability from the fuel tank resulting in slight increase of flammability exposure within the given tank	None	None	MINOR	1.00E-05

Annunciated loss of sufficient nitrogen enriched air supply to the fuel tank	ALL	Reduction in oxygen displacement capability from the fuel tank resulting in slight increase of flammability exposure within the given tank	Inerting system failure message	None	MINOR	1.00E-05
Function: Limit the rate of Nitrogen Enriched Air supply into fuel tanks to prevent over pressurization of fuel						
Type of Hazard	Flight Phase	Effect on Aircraft	Pilot Recognition Method	Pilot Action	Criticality	Safety Requirement
Supply of high pressure air to the fuel tank	ALL	Slight airflow rate change within the fuel tank with no effect on system operation	None	None	MINOR	1.00E-05
Function: Provide High Temperature Protection of Nitrogen Enriched Air supply to the fuel tanks						
Type of Hazard	Flight Phase	Effect on Aircraft	Pilot Recognition Method	Pilot Action	Criticality	Safety Requirement
Supply of unregulated hot air to the fuel tank	ALL	Potential fire hazard	None	None	CATASTROPHIC	1.00E-09

<table>
<tr><td colspan="7">Function: Prevent Reverse Flow of fuel or fuel vapor from the fuel tanks into the FTIS</td></tr>
<tr><td>Type of Hazard</td><td>Flight Phase</td><td>Effect on Aircraft</td><td>Pilot Recognition Method</td><td>Pilot Action</td><td>Criticality</td><td>Safety Requirement</td></tr>
<tr><td>Reverse airflow causing fuel vapors coming in contact with ignition sources</td><td>ALL</td><td>Potential fire hazard</td><td>None</td><td>None</td><td>CATASTROPHIC</td><td>1.00E-09</td></tr>
</table>

The FAA[14] provides the following criticality guidance for airborne systems:

Criticality Definitions:

- Catastrophic: failure conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane
- Minor: failure conditions that would not significantly reduce airplane safety and involve crew actions that are within their capabilities

Frequency of Occurrence:

- Catastrophic: must be Extremely Improbable with Events per Hour occurring less than once during one billion flight hours ($1x10^{-9}$)
- Minor: must be Remotely Probable with Events per Hour occurring less than once during one hundred thousand flight hours ($1x10^{-5}$)

An avionics certification reference guide used widely at Honeywell Aerospace[15] quotes the FAA on page 4-15: "the probability should be established as a risk per hour in a flight where the duration is equal to the expected mean flight time and for the airplane. For example, in systems where the hazard results from multiple failures in the same flight, the numerical assessment should take account of the likelihood that this will occur in a flight of expected average duration. Similarly, in those cases where failures are only critical for a particular period of flight, the hazard may be averaged over the whole of the expected mean flight time". This statement from the FAA is intended to

[14] FAA Advisory Circular 23.1309-1A

[15] Validating Digital Systems in Avionics and Flight Control, Avionics Communications Inc., 1993

give some relief to suppliers of systems that don’t operate throughout the entire flight regime, an example is a landing gear system.

In the case of inerting systems, the percentage of flight time that the FTIS operates is determined by the aircraft manufacturer and based on the aircraft’s construction. For aircraft of conventional construction, such as the Boeing 747, the wing (and therefore the fuel tanks) is formed by sheets of aluminum attached to ribs and spars. The aluminum “skin” of the wing conducts heat so well that during flight, where the Outside Air Temperature[16] at cruise altitude of 35,000 feet is typically -55°C, there is little need to add nitrogen to the ullage because the fuel tanks have been inerted by the low temperatures. As per FAR 25.1309 Appendix N[17] which governs the requirements for conducting fuel tank flammability exposure analyses for Transport Category Aircraft: “For fuel tanks installed in aluminum wings, a qualitative assessment is sufficient if it substantiates that the tank is a conventional unheated wing tank”. In other words, just the fact the aircraft’s fuel tank is located in an aluminum wing means that tank is considered inerted by virtue of its exposure to low temperatures and no additional inerting (such as Nitrogen) is required. This statement in Appendix N allows aircraft of conventional construction to get by with adding an inerting system just for the center fuel tank, which is the tank that exploded in the TWA 800 Boeing 747.

In the case of more modern aircraft, such as the Bombardier CSeries or Boeing’s 787, the wing is constructed of a carbon fiber composite material which acts like a Thermos bottle and maintains a relatively high fuel temperature. Realizing that one of the disadvantages to a carbon fiber wing is higher average fuel temperatures,

[16] Pilot’s Handbook of Aeronautical Knowledge, Federal Aviation Administration, 2009

[17] Code of Federal Regulations, Title 14, Chapter I, Subchapter C, Part 25, Subpart I, Appendix N

Bombardier added the following requirement to its customer requirements document: BA-500-04: The FTIS shall be capable of providing NEA during any aircraft operating phase. Because the trend in new aircraft design is toward more efficient but more insulative composites such as carbon fiber, for this study of various FTIS architectures it will be assumed the inerting system will be operational throughout all flight phases.

To meet the criticality requirements listed in the sample SFHA, fuel tank inerting systems and their safety features must be extremely reliable. FTIS safety features include pressure and temperature sensors, safety valves, check valves, j-trap and certain software algorithms in the controller. These safety-related items are seen in the Block Definition Diagrams; Figures 10, 11, and 12.

<u>Development and Design Assurance Levels</u>

For an airborne system function to be considered as meeting a particular reliability number, such as only one failure allowed in one hundred thousand flight hours ($1x10^{-5}$), a safety study must be performed per ARP-4761[18]. This safety study will assign a Function Development Assurance Level (FDAL) to each component in the system. For software development the process requirements outlined in DO-178B[19] must be strictly followed, which involves a large number of process documents for higher criticality levels and at least four FAA audits. DO-178B carries five Item Design Assurance Levels (IDAL), shown in Table 7. In accordance with Section 5.2.3 of ARP4754A these IDALs must align with the FDALs determined by the ARP4761 safety

[18] SAE Aerospace ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

[19] Software Considerations in Airborne Systems and Equipment Certification, Radio Technical Commission on Aeronautics, Document 178 Revision B

analysis. This table contains criticality descriptions quoted from another Avionics Communications[20] publication utilized by Honeywell Aerospace for avionics certification.

Table 7: Failure Mode Criticality Definitions

Item Design Assurance Level	Failure Mode Criticality	Criticality Definition
A	Catastrophic	Failure conditions which would prevent continued safe flight and landing
B	Hazardous	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: 1. A large reduction in safety margins or functional capabilities OR 2. Physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or complexly OR 3. Adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants
C	Major	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: 1. A significant reduction in safety margins or functional capabilities OR 2. A significant increase in crew workload or in conditions impairing crew efficiency OR 3. Discomfort to occupants, possibly including injuries.

[20] Performing a Safety Certification for Avionics Components and Systems, Avionics Communications, Inc, 1995

Item Design Assurance Level	Failure Mode Criticality	Criticality Definition
D	Minor	Failure conditions which would not significantly reduce aircraft safety and which would involve crew actions that are well within their capabilities. Minor failure conditions may include: 1. A slight reduction in safety margins or functional capabilities OR 2. A slight increase in crew workload such as routine flight plan changes OR 3. Some inconvenience to passengers
E	No Effect	Failure conditions which do not affect the operational capability of the aircraft or increase pilot workload

The three fuel tank inerting systems studied in this thesis paper would be assigned different FDALs and IDALs:

- Architecture #1: Onboard Storage – FDAL/IDAL D

  Minor Criticalities:

  - Unannunciated loss of sufficient nitrogen enriched air supply to the fuel tank
  - Annunciated loss of sufficient nitrogen enriched air supply to the fuel tank
  - Supply of high pressure air to the fuel tank

- Architecture #2: Bleed Air – FDAL/IDAL A

  Minor Criticalities:

  - Unannunciated loss of sufficient nitrogen enriched air supply to the fuel tank
  - Annunciated loss of sufficient nitrogen enriched air supply to the fuel tank
  - Supply of high pressure air to the fuel tank

Catastrophic Criticalities:

  - Supply of unregulated hot air to the fuel tank
  - Reverse airflow causing fuel vapors coming in contact with ignition sources

- Architecture #3: Compressor – FDAL/IDAL A

  Minor Criticalities:

  - Unannunciated loss of sufficient nitrogen enriched air supply to the fuel tank
  - Annunciated loss of sufficient nitrogen enriched air supply to the fuel tank
  - Supply of high pressure air to the fuel tank

  Catastrophic Criticality:

  - Reverse airflow causing fuel vapors coming in contact with ignition sources

The Onboard Storage method (Architecture #1) gets a large relief from the SFHA criticalities because neither of the Catastrophic hazards apply to this type of system; "Supply of unregulated hot air to the fuel tank" does not apply because this architecture does not utilize a source of hot air, and "Reverse airflow causing fuel vapors coming in contact with ignition sources" does not apply because a source of ignition (the oxygen sensor used in the other architectures) isn't necessary in the Onboard Storage method. The ARP4761 safety analysis assigns an FDAL of D to this architecture. The software IDAL will follow suit with an IDAL D, per DO-178B.

The Bleed Air method of generating NEA on board the aircraft (Architecture #2) is assigned an A FDAL because Section 5.2.1 of ARP4754A provides the following assignment principle: "If a Catastrophic Failure Condition (FC) could result from a possible development error in an aircraft/system function or item, then the associated Development Assurance process is assigned level A". The ARP4761 safety analysis finds that either software or hardware failures in this system architecture could result in both of the SFHA-identified Catastrophic FCs therefore this architecture receives an FDAL/IDAL of A.

The Compressor method of generating NEA on board the aircraft (Architecture #3) is likewise assigned an A FDAL/IDAL because the ARP4761 safety analysis finds that either software or hardware failures in this system architecture could result in the SFHA-identified Catastrophic FC of “Reverse airflow causing fuel vapors coming in contact with ignition sources”.

This FC is identified as a failure hazard for both the Onboard Storage and Compressor FTIS Architectures because they both utilize an oxygen sensor to check that the oxygen concentration of the NEA exiting the ASM is below the level required to maintain an inert fuel tank. Within the oxygen sensor is a Zirconium sensor element that operates at 700°C which will ignite jet fuel or vapors from the fuel tank.

FDAL/IDAL Contribution to System Development Level of Effort

As per ARP4754A, the development of each FTIS component must be accompanied by documentation according to its FDAL/IDAL, hereafter referred to simply as DAL. Table 8 is an example of the differences in the required Validation documents required for various DALs and is taken from Section 5.4.6.1 of ARP4754A.

Table 8: Requirements Validation Methods and Data

Methods and Data	Development Assurance Level A and B	Development Assurance Level C	Development Assurance Level D	Development Assurance Level E
PASA/PSSA	R	R	A	N
Validation Plan	R	R	A	N
Validation Matrix	R	R	A	N
Validation Summary	R	R	A	N
Requirements Traceability (Non-Derived Requirements)	R	R	A	N
Requirements Rationale (Derived Requirements)	R	R	A	N
Analysis, Modeling, or Test	R	One recommended	A	N
Similarity (Service Experience)	A		A	N
Engineering Review	R		A	N

R - Recommended for certification, A - As negotiated for certification, N - Not required for certification

Other sets of documents required or not required, according to the component's DAL, by ARP4754A are Safety Assessment Process, Verification Methods and Data, Configuration Management Activities, Process Assurance Plans and Reviews, Aircraft and System Development Process and Requirements Capture, and Planning Process. Documents marked as A (As negotiated for certification) are typically not required from well-established aircraft system developers.

As the governing publication for airborne software development, DO-178B, which mimics ARP4754A in its process requirements methodology, has an additional and very large list of documentation that is necessary to produce. Adhering to the DO-178B process is necessary for every component that contains software.

Another RTCA publication is DO-254, which is virtually identical to DO-178B but is intended to apply to Complex Electronic Hardware (CEH) which can fulfill the same function a microprocessor (or microcontroller) executing software. The CEH is loaded with operational code just once, vs. a microprocessor which continuously cycles through code that was loaded into electronic memory. The intent of both DO-178B and DO-254 is to assure the certifying authorities that a sufficient level of rigor was applied during the software development process that the reliability number (such as 10^{-9} failures per flight hour) assigned to that software is ensured. Because DO-178B and DO-254 require the same level of documentation effort, an FTIS component that contains both a microprocessor and a CEH device will double the considerable amount of development and process documentation necessary. For a DAL D component this level of effort could be reasonable but for a DAL A or B it likely would be considered onerous.

These RTCA and SAE process documents and their resulting activity requirements, such as safety studies, software audits, independent reviews, peer reviews, environmental tests, etc., have a multiplicative effect on the level of effort required for FAA certification. In the book Avionics Certification[21] (Chapter 28: Cost Estimation and Metrics), Vance Hilderman and Tony Baghai describe DAL D certification as having hardly any additional effort than a non-certified project because DAL D is comprised almost entirely of normal industry standard engineering principles. DAL C, B and A increase project development cost by 60% to 80%, claim Hilderman

[21] Avionics Certification, V. Hilderman & T. Baghai, 2007

and Baghai, which they point out is the industry average. Presumably the author's opinion is that the DAL C increase is 60% and for DAL A the increase is 80%. Appendix A, B and C contain tables from ARP4754A, DO-178B, and DO-254 that list which documents are recommended (required) for each DAL.

A tally of the ARP4754A required documents has DAL D at 15 and DAL A at 47, with 18 of these subject to an independent process requirement. Process independence entails adding a resource to the project, further increasing system development costs. An example of process independence is given in Section 5.4.5 of ARP4754A, Validation Rigor: "The most common means of achieving independence in requirements validation is an independent review of requirement data and supporting rationale to determine if there is sufficient evidence to argue the correctness of a requirement and the completeness of a set of requirements". Process independence for other ARP4754A required documentation is similar.

For DO-178B, required documents total 80 For DAL A, including 25 that require process independence while DAL D needs just 38 documents and only 2 are subject to the independence requirement. The DO-254 documentation requirements are fewer, but with similar proportions: 27 required documents for DAL A and 13 for DAL D plus 3 partial document requirements. For DO-254 no process independence is necessary.

In addition to the various DALs requiring different levels of effort in the numbers of documents, as the documents are produced they are subject to different levels of Configuration Management (CM) controls, categorized as System Control 1 or System Control 2 for ARP4754A and shown in Table 9. Table 10 contains the software CM controls required by DO-178B and Table 11 has the similar hardware controls for DO-254.

Table 9: CM Activities to Control Category Mapping for ARP4754A

CM Process Activity	System Control Category 1	System Control Category 2
Configuration Identification	X	X
Configuration Baseline(s) Establishment	X	
Problem Reporting	X	
Change Control – Integrity assurance	X	X
Change Control – Tracking	X	
Configuration Index Establishment	X	X
Archive and Retrieval	X	X

Table 10: SCM Activities to Control Category Mapping for DO-178B

SCM Process Activity	Software Control Category 1	Software Control Category 2
Configuration Identification	X	X
Baseline(s)	X	
Traceability	X	X
Problem Reporting	X	
Change Control – Integrity and Identification	X	X
Change Control – Tracking	X	
Configuration Status Accounting	X	X
Archive and Retrieval	X	X
Protection against Unauthorized Changes	X	X
Media Selection, Refreshing, Duplication	X	
Release	X	
Data Retention	X	X

Table 11: HCM Activities to Control Category Mapping for DO-254

HCM Process Activity	Hardware Control Category 1	Hardware Control Category 1
Configuration Identification	X	X
Baseline(s)	X	
Baseline Traceability	X	X
Problem Reporting	X	
Change Control – Integrity and Identification	X	X
Change Control – Records, Approvals and Traceability	X	
Release	X	
Archive and Retrieval	X	X
Data Retention	X	X
Protection against Unauthorized Changes	X	X
Media Selection, Refreshing, Duplication	X	

As shown in the Appendices, even DAL D requires some amount of CM but as can be expected, DAL A requires a much higher level of CM effort. Of the 47 documents ARP4754A requires for a DAL A system, 20 are expected to adhere to Control Category (CC) 1 standards and the other 27 are subject to CC 2. DAL D system documentation, per ARP4754A, has just 2 documents under CC1 and 13 under CC2. For DAL A software documents (DO-178B), 26 use CC1 SCM process activities and the other 54 use CC2 while DAL D software documents have 10 using CC1 and 28 using CC2. Dal A hardware documents are divided into 10 for CC1, 17 for CC2 and for DAL D, 7 use CC1 and 9 use CC2.

CONCLUSIONS

This thesis paper has examined two major aspects of developing an FTIS: requirements compliance and system complexity. Fifteen customer-level requirements from the Bombardier CSeries commercial airliner program were analyzed for each of three FTIS architectures. For system complexity, Design and Development Assurance Levels were utilized to arrive at a quantifiable comparison.

Customer Requirements Coverage

The score for each system architecture's ability to meet customer requirements is shown in Table 12.

Table 12: Customer Requirements Coverage by Architecture

Number of Customer-level Requirements	Architecture #1: Onboard Storage	Architecture #2: Bleed Air	Architecture #3: Compressor
Complied With	9	14	13
Not Applicable	4	0	0
Not Complied With	2	1	2

All three systems fail to meet this customer-level requirement: *BA-500-12: The FTIS shall be controlled by solid-state devices*. In the requirements decomposition process this requirement was flowed down to two system-level requirements; *FTIS-005: Power for all electrical FTIS components, valve on/off and flow control shall be provided by a microprocessor or microcontroller working in conjunction with solid-state devices* and *FTIS-006: The FTIS shall not contain electromechanical devices such as micro* *switches or relays*. All three FTIS architectures comply with FTIS-005 but not FTIS-006, therefore all three fail to comply with BA-500-12.

The reason FTIS-006 is not met by any of these FTIS architectures is they all contain valves that utilize micro switches for valve position feedback. Shown in the Tracing and Notes column of Table 1, for FTIS-006, is this comment “Bombardier’s concern is with system reliability so Hall-effect sensors may be necessary for detecting valve position”. This comment would have been recorded during a system design review held with the customer, in this case Bombardier, which is part of the process of flowing down (decomposing) customer requirements to system requirements.

Unfortunately, very high levels of electromagnetic environmental tests are being imposed on newly designed aircraft that utilize composite construction, such as carbon fiber, because composites do not shield against this type of energy as well as metal. The Hall-effect sensors that Bombardier wanted to see included in the valves’ design were adversely affected during these environmental tests and had to be replaced with mechanical micro switches even though this violated BA-500-12. In this case, the customer will have to consider the requirement as partially complied with and not reject any of the FTIS architectures because of it.

The customer-level requirement that Architectures #1 & #3 are not in compliance with is *BA-500-07: The FTIS system Guaranteed Not to Exceed Weight (GNTEW) shall not exceed 75 lbs dry weight (structures mounting bracketry not included)*. This requirement can only be met by an on-board Nitrogen generating FTIS that connects to a readily available source of hot and relatively clean pressurized air, which is Architecture #2. This weight advantage is why aircraft manufacturers such as Airbus, Boeing, Bombardier, COMAC and Sukhoi have chosen Architecture #2 for their latest commercial aircraft, even while the durability of HFM technology is not yet proven.

System Complexity

A system safety analysis was performed for each FTIS architecture with this result:

- Architecture #1: Onboard Storage – DAL D
- Architecture #2: Bleed Air – DAL A
- Architecture #3: Compressor – DAL A

Both the system developer and the aircraft manufacturer should carefully consider whether the advantage of saving a few pounds of overall system weight can be negatively offset by the huge difference in the level of development effort when comparing DAL D and DAL A systems. The differences in documentation and process requirements is compiled in Tables 13, 14, and 15.

Table 13: System Documentation Required per ARP4754A

FTIS Architecture	System Control Category 1	System Control Category 2	Total Number of Required Documents
#1: Onboard Storage	2	13	15 (0 with process independence)
#2: Bleed Air	20	27	47 (18 with process independence)
#3: Compressor	20	27	47 (18 with process independence)

Table 14: Software Documentation Required per DO-178B

FTIS Architecture	Software Control Category 1	Software Control Category 2	Total Number of Required Documents
#1: Onboard Storage	10	28	38 (2 with process independence)
#2: Bleed Air	26	54	80 (25 with process independence)
#3: Compressor	26	54	80 (25 with process independence)

Table 15: Hardware Documentation Required per DO-254

FTIS Architecture	Hardware Control Category 1	Hardware Control Category 2	Total Number of Required Documents
#1: Onboard Storage	7	9	16
#2: Bleed Air	10	17	27
#3: Compressor	10	17	27

Of all the configuration management activities, Problem Reporting and Change Control involve the most resources and a correspondingly high level of effort. Whether the CM is for System, Software or Hardware documentation, the magnitude of these two activities causes CC1 to entail at least three times the effort of CC2. This has been my experience at both Honeywell Aerospace and Parker Aerospace, because typically a formal Change Control Board (CCB) is assigned to the project to manage these two CM activities.

Because Process Independence requires an independent review of the documentation, along with the subsequent back-and-forth between the document's author and reviewer, a factor of two can be entered for the effort needed to complete all documents subject to this requirement.

Factoring in the CM activities allows a quantifiable approximation of the differences in the effort necessary to develop and maintain documentation for each FTIS architecture.

Table 16: System Documentation Effort Required per ARP4754A

FTIS Architecture	System Control Category 1	System Control Category 2	Documents Subject to Process Independence	Documentation Effort
#1: Onboard Storage	2(3)=6	13	0	19
#2: Bleed Air	20(3)=60	27	18(2)=36	123
#3: Compressor	20(3)=60	27	18(2)=36	123

Table 17: Software Documentation Effort Required per DO-178B

FTIS Architecture	Software Control Category 1	Software Control Category 2	Documents Subject to Process Independence	Documentation Effort
#1: Onboard Storage	10(3)=30	28	2(2)=4	62
#2: Bleed Air	26(3)=78	54	25(2)=50	182
#3: Compressor	26(3)=78	54	25(2)=50	182

Table 18: Hardware Documentation Effort Required per DO-254

FTIS Architecture	Hardware Control Category 1	Hardware Control Category 2	Documents Subject to Process Independence	Documentation Effort
#1: Onboard Storage	7(3)=21	9	0	30
#2: Bleed Air	10(3)=30	17	0	47
#3: Compressor	10(3)=30	17	0	47

As a recap, the following list summarizes the documentation effort for each FTIS architecture:

- Architecture #1: Onboard Storage
    - System – 19
    - Software – 62
    - Hardware – 30
        - Total Documentation Effort = 111
- Architecture #2: Bleed Air and Architecture #3: Compressor
    - System – 123
    - Software – 182
    - Hardware – 47
        - Total Documentation Effort = 352

The amount of engineering man-hours required just for documenting Architectures #2 or #3 is three times that of Architecture #1, a major consideration for the project's managers when choosing an FTIS.

Closing Remarks

Repeated from the Abstract: when choosing a system architecture, requirements analysis is often overlooked and documentation workload is brushed aside in favor of purely technical analyses.

This thesis paper has demonstrated why a thorough requirements analysis must be performed for each system architecture being considered, early in the project management process. Without this analysis an unknown risk will exist within the project that may not be discovered until many thousands of engineering man-hours have been expended. Armed with an analysis of requirements, performed by utilizing the use case method demonstrated in this paper, the project's manager or system engineer can see a possible risk event whose impact might be mitigated, possibly by renegotiating the requirements with the customer.

Failing a requirements renegotiation an alternative architecture could be chosen relatively quickly if a comparative requirements analysis has been performed; again and very importantly, early in the planning stage of the project. For example, if Architecture #1 was initially chosen and the customer refused to give relief on the weight requirement that system would not meet, FTIS Architecture #2 could be quickly proposed as an alternative provided the non-compliance requirements for that system were acceptable to the customer.

It should be noted here that to maintain focus on the principle being explained, in this thesis paper the Bombardier customer-level requirements were kept to the most important 15 requirements. The actual Bombardier BD-500 Inerting System Technical Requirements Document numbers 73 pages and contains a few hundred requirements.

A thoroughly analyzed requirements matrix of these three FTIS architectures undoubtedly would reveal each type of FTIS is non-compliant with at least a few customer-level requirements.

Beyond the risks of developing an FTIS that may not be compliant with customer-level requirements is the quantifiable difference in each architecture's level of effort. An experienced project manager or system engineer can easily sum the number of system components from a bill of materials and estimate the number of engineering man-hours necessary to meet the technical system requirements (usually from previously developed similar components) but typically the documentation effort is not given a second thought.

As part of the FTIS architecture selection process, a documentation level of effort analysis must also be performed – again early in the project management process. This would be a project management advantage if choosing one FTIS architecture over another would entail a substantial effort in redesigning or creating a newly designed system component. For example, if choosing Architecture #1 required a large level of effort to design a new method of LN_2 storage this could be justified (i.e. offset) by the much lower level of engineering effort in producing the required documentation.

Recommendations

Gathering an understanding of the various FTIS architectures from the reference materials used while researching for this thesis paper, the following recommendations can be made:

- Architecture #1: Onboard Storage. Best for aircraft expected to have rapid descents as part of the normal flight regime. This can include aircraft involved with military operations or commuter jets striving for maximum efficiency, since a jet-powered aircraft is much more efficient with fuel while at a cruising altitude. Additional advantages are the least complexity and the lowest level of documentation effort.

- Architecture #2: Bleed Air. Best at fulfilling the civil transport aircraft manufacturer's two most critical requirements: low system weight and meeting the FAR 25.981 inerting thresholds. If Monte Carlo analysis shows this FAR can be met with a single ASM, this architecture will be the consistent winner. Disadvantages are high system complexity and level of documentation effort.
- Architecture #3: Compressor. Midway between the other two FTIS architectures with less weight that Architecture #1 and less complexity than Architecture #2. May be the FTIS architecture of choice if the aircraft's bleed air system cannot supply enough bleed air flow or pressure. Disadvantage is a level of documentation effort matching Architecture #2.

A trend toward higher fuel efficiency in modern airliners may make choosing between FTIS Architectures easier. Tapping bleed air from a turbine engine reduces its power output slightly so allocation of this precious source of hot pressurized air to the various aircraft systems requiring it is carefully controlled. Some of these systems need the (greater than) 200°C heat energy, such as the wing anti-ice system, but the compressor in FTIS Architecture #3 provides enough heat energy from the heat of compression to operate an ASM adequately. As the airliner manufacturers become stingier with bleed air, the viability of FTIS Architecture #2 begins to fail.

Another airliner trend is less main engine operating time to save fuel. An auxiliary engine, the Auxiliary Power Unit (APU), is utilized while the airliner is parked at the boarding gate being prepared for flight. The APU is a very small turbine engine, just large enough to power some electrical systems such as cabin air conditioning. The predicted trend is to also depend on just the APU while the aircraft is moved to the end of the runway, either by a tow vehicle or by electric motors within the wheels. Honeywell recently demonstrated an electric taxi system[22] in Toulouse, France on an Airbus A320 where the expectation is that environmental regulations will not allow main engine taxi operations within a few years at some European Union airports. Because an APU cannot provide adequate bleed air pressure to operate an ASM, the trending practices of airline operation will drive the need for FTIS Architecture #3 over #2.

At the time this thesis paper was written, in 2014, the Bleed Air method of FTIS Architecture #2 was most popular among the major airliner manufacturers because it met their needs. Changes in environmental regulation, an increasing price of jet fuel, or alterations in an airline's operations could easily increase the viability of either the Compressor or On Board Storage methods of maintaining inerted fuel tanks in airliners.

[22] http://www.greentaxiing.com/: Introducing EGTS™, the future of aircraft taxiing

REFERENCES

Avionics Communications Inc., (1993). *Validating Digital Systems in Avionics and Flight Control*. Leesburg, VA: Author.

Avionics Communications Inc., (1995). *Performing a Safety Certification for Avionics Components and Systems.* Leesburg, VA: Author.

Burns, M., Cavage, W.M., Hill, R., Morrison, R. (2004). *Flight-Testing of the FAA Onboard Inert Gas Generation System on an Airbus A320* (DOT/FAA/AR-03/58). Retrieved from http://www.fire.tc.faa.gov/pdf/03-58.pdf

Burns, M., Cavage, W.M., Morrison, R., Summer, S. (2004). *Evaluation of Fuel Tank Flammability and the FAA Inerting System on the NASA 747 SCA* (DOT/FAA/AR-04/41). Retrieved from http://www.fire.tc.faa.gov/pdf/04-41.pdf

Cavage, W.M., Morrison, R., (2004) *Development and Testing of the FAA Simplified Fuel Tank Inerting System.* Retrieved from http://www.fire.tc.faa.gov/pdf/systems/Cavage-FAAOBIGGSDevelop&Test.pdf

Cavage, W.M., Morrison, R., (2004). *Development and Testing of the FAA Simplified Fuel Tank Inerting System, a PowerPoint presentation.* Retrieved from http://www.fire.tc.faa.gov/ppt/systems/FAAOBIGGSDevelopment&Test.ppt

Cherry, R., Warren, K. (1999). *A Benefit Analysis for Nitrogen Inerting of Aircraft Fuel Tanks Against Ground Fire Explosion* (DOT/FAA/AR-99/73). Washington, D.C.: Office of Aviation Research.

Clodfelter, R. G., Anderson, C.L., Vannice, W.L. (1987). *OBIGGS For Fighter Aircraft* (SAE Technical Paper Series 871903). Retrieved from http://papers.sae.org/871903/

EGTS International. (2014, June). *Pilots test drive "remarkable innovation" during EGTS™ Pilots Days* (Press Release). Toulouse, France: Author.

Federal Aviation Administration Advisory Circular 25.1309-1A *System Design and Analysis* (1988). *Retrieved from http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/22680*

Federal Aviation Administration Advisory Circular 25.981-2A *Fuel Tank Flammability Reduction Means* (2008). Retrieved from http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/list/AC%2025.981-2A/$FILE/AC%2025.981-2A.pdf

Federal Aviation Administration Fact Sheet – *Fuel Tank Safety*, (2006). Retrieved from https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=7318

Fuel Tank Flammability Exposure and Reliability Analysis, 14CFR, Chapter I, Subchapter C, Part 25, Subpart I, Appendix N (2011). Retrieved from http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=14%3A1.0.1.3.11#ap14.1.25_11801.n

Hilderman, V., Baghai, T., (2007). *Avionics Certification: a complete guide to DO-178B (software), DO-254 (hardware).* Leesburg, VA: Avionics Communications Inc.

Holt, J., Perry, S. (2008). *SysML for Systems Engineering.* London, United Kingdom: The Institution of Engineering and Technology.

Klueg, E. P., McAdoo, W. C., & Neese, W. F. (1972). *Performance of a DC-9 Aircraft Liquid Nitrogen Fuel Tank System* (FAA-RD-72-53). Retrieved from http://www.fire.tc.faa.gov/pdf/rd72-53.pdf

Radio Technical Commission on Aeronautics, Standards and Guidance Materials (2000). *Design Assurance Guidance for Airborne Electronic Hardware*, (DO-254). Washington, D.C.: RTCA, Inc.

Radio Technical Commission on Aeronautics, Standards and Guidance Materials (1992). *Software Considerations in Airborne Systems and Equipment Certification*, (DO-178B). Washington, D.C.: RTCA, Inc.

The Society of Automotive Engineers, Aerospace Recommended Practice (1996). *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment* (ARP4761). Retrieved from http://standards.sae.org/arp4761/

The Society of Automotive Engineers, Aerospace Recommended Practice (2010). *Guidelines for Development of Civil Aircraft and Systems* (ARP4754A). Retrieved from http://standards.sae.org/arp4754a/

U.S. Department of Transportation, Federal Aviation Administration, Flight Standards Service (2008). *Pilot's Handbook of Aeronautical Knowledge* (FAA-H-8083-25A). Retrieved from https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/pilot_handbook/

Zinn, S. V., Jr. (1971). *Inerted Fuel Tank Oxygen Concentration Requirements* (FAA-RD-71-42). Retrieved from http://www.fire.tc.faa.gov/pdf/rd7142.pdf

APPENDIX A: ARP4754A PROCESS OBJECTIVES DATA AND SYSTEM CONTROL CATEGORIES[23]

[23] Excerpted from: SAE Aerospace ARP4754A: Guidelines for Development of Civil Aircraft and Systems

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
1.0 Planning Process														
1.1	System development and integral processes activities are defined	5.8.1 5.8.4.1	R	R	R	R	R	Certification Plan	①	①	①	①	①	
		3.1 5.1.5 Appx B	R	R	R	R	N	Safety Program Plan	②	②	②	②		
		3.1 5.8.4.3	R	R	R	R	N	Development Plan	②	②	②	②		
		5.4.2a 5.4.7.1	R	R	R	A	N	Validation Plan	②	②	②	②		
		5.5.3 5.5.5.1	R	R	R	A	N	Verification Plan	②	②	②	②		
		5.6.2.1	R	R	R	R	A	Configuration Management Plan	②	②	②	②		
		5.7.2	R	R	R	R	N	Process Assurance Plan	②	②	②	②		
1.2	Transition criteria and inter-relationship among processes are defined.	3.2	R	R	R	A	N	Plans in objective no. 1	②	②	②	②		
R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification. * Independence is achieved when the activity is performed by a person(s) other than the developer of the system/item.														

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
2.0 Aircraft and System Development Process and Requirements Capture														
2.1	Aircraft-level functions, functional requirement, functional interfaces and assumptions are defined	4.1.4 4.2 5.3	R	R	R	R	N	List of Aircraft-level functions Aircraft-level Requirements	①	①	①	②		Note: Requirements capture process objectives presented in section 5.3 are included in this development process
2.2	Aircraft functions are allocated to systems	4.1.5 4.3	R	R	R	R	N	System Requirements	①	①	①	②		
2.3	System requirements, including assumptions and system interfaces are defined.	5.3	R	R	R	R	N	System Requirements	①	①	①	②		
2.4	System derived requirements (including derived safety-related requirements) are defined and rationale explained.	4.4 5.3.1.4 5.3.2	R	R	R	A	N	System Requirements	①	①	①	②		
2.5	System architecture is defined.	4.1.6 4.4 5.8.4.4	R	R	R	A	N	System Design Description	①	①	②	②		
2.6	System requirements are allocated to the items.	4.1.7 4.5 4.6 5.3	R	R	R	R	N	Item Requirements	①	①	①	②		
2.7	Appropriate item, system and aircraft integrations are performed.	4.6.3 4.6.4	R	R	R	A	N	Verification Summary	②	②	②	②		

R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.
* Independence is achieved when the activity is performed by a person(s) other than the developer of the system/item.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
3.0 Safety Assessment Process														
3.1	The aircraft/system functional hazard assessment is performed.	5.1.1 5.2.3 5.2.4	R*	R*	R	R	R	Aircraft FHA System FHA	①	①	①	①	①	
3.2	The preliminary aircraft safety assessment is performed.	5.1.2 5.2.3 5.2.4	R*	R*	R	A	N	PASA	①	①	①	①		
3.3	The preliminary system safety assessment is performed.	5.1.2 5.1.6 5.2.3 5.2.4	R*	R*	R	A	N	PSSA	①	①	①	②		
3.4	The common cause analyses are performed.	5.1.4	R	R	A	N	N	Particular Risk Assessment	①	①	①			
			R*	R*	A	N	N	Common Mode Analysis	①	①	①			
			R	R	A	N	N	Zonal Safety Analysis	①	①	①			
3.5	The aircraft safety assessment is performed.	5.1.3 5.1.6	R*	R*	R	A	N	ASA	①	①	①	①		
3.6	The system safety assessment is performed.	5.1.3 5.1.6	R*	R*	R	A	N	SSA	①	①	①	②		
3.7	Independence requirements in functions, systems and items are captured	5.3.2 5.2.3 5.1.2	R*	R*	R	R	N	System, HW, SW Requirements PASA PSSA	①	①	①	②		

R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.
* Independence for the safety artifacts is achieved when the safety activity is performed by a person(s) other than the developer of the system/item.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	**Objective Description**		**A**	**B**	**C**	**D**	**E**		**A**	**B**	**C**	**D**	**E**	
4.0 Requirements Validation Process														
4.1	Aircraft, system, item requirements are complete and correct.	5.4 5.4.2 c 5.4.3 5.4.4	R*	R*	R	A	N	Validation Results	②	②	②	②		Includes coordination of interfaces between systems and between items.
4.2	Assumptions are justified and validated	5.4.2.d	R*	R	R	A	N	Validation Results	②	②	②	②		
4.3	Derived requirements are justified and validated.	5.3.1.4 5.3.2 5.4.2	R*	R*	R	A	N	Validation Results	②	②	②	②		
4.4	Requirements are traceable.	5.4.3 5.4.4	R	R	R	A	N	Validation Results	②	②	②	②		
4.6	Validation compliance substantiation is provided.	5.4.2.e 5.4.2.f 5.4.8 5.4.7.4	R	R	R	A	N	Validation Summary (including Validation Matrix)	②	②	②	②		

R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.
* Independence for the requirement artifacts is achieved when the validation activity is performed by a person(s) other than the developer of the requirement.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
5.0 Implementation Verification Process														
5.1	Test or demonstration procedures are correct.	5.5.4.3	R*	R	R	A	N	Verification Procedures	①	①	②	②		
5.2	Verification demonstrates intended function and confidence of no unintended function impacts to safety.	5.5.1 5.5.5.3 5.5.5.2	R*	R	R	A	N	Verification Procedures	①	①	②	②		
			R*	R	R	A	N	Verification Results	②	②	②	②		
5.3	Product implementation complies with aircraft, and system requirements.	5.5.1 5.5.2	R*	R	R	A	N	Verification Procedures	①	①	②	②		
			R*	R	R	A	N	Verification Results	②	②	②	②		Specific item verification activities are performed under DO-178B/ED-12B and DO-254/ED-80.
5.4	Safety requirements are verified.	5.5.1 5.5.5.3	R*	R*	R	A	N	Verification Procedures and Results (ASA, SSA)	②	②	②	②		See Appendix A, Section 3.0, Safety Assessment Objectives for specific safety objectives and control categories.
5.5	Verification compliance substantiation is included.	5.5.6.3	R	R	R	A	N	Verification Matrix	②	②	②	②		
		5.5.6.4	R	R	R	A	N	Verification Summary	②	②	②	②		
5.6	Assessment of deficiencies and their related impact on safety is identified.	5.5.6.4	R	R	R	A	N	Verification Summary	②	②	②	②		
			R	R	R	A	N	Problem Reports	②	②	②	②		

R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.
* Independence is achieved when the verification activity is performed by a person(s) other than the developer.

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
6.0 Configuration Management Process														
6.1	Configuration items are identified.	5.6.2.2	R	R	R	A	N	CM Records	②	②	②	②		
6.2	Configuration baseline and derivatives are established.	5.6.2.3	R	R	R	A	N	Configuration Baseline Records	①	①	②	②		
6.3	Problem reporting, change control, change review, and configuration status accounting are established.	5.6.2.4	R	R	R	R	N	Problem reports CM Records	②	②	②	②		
6.4	Archive and retrieval are established.	5.6.2.5	R	R	R	R	N	CM Records	②	②	②	②		
R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.														

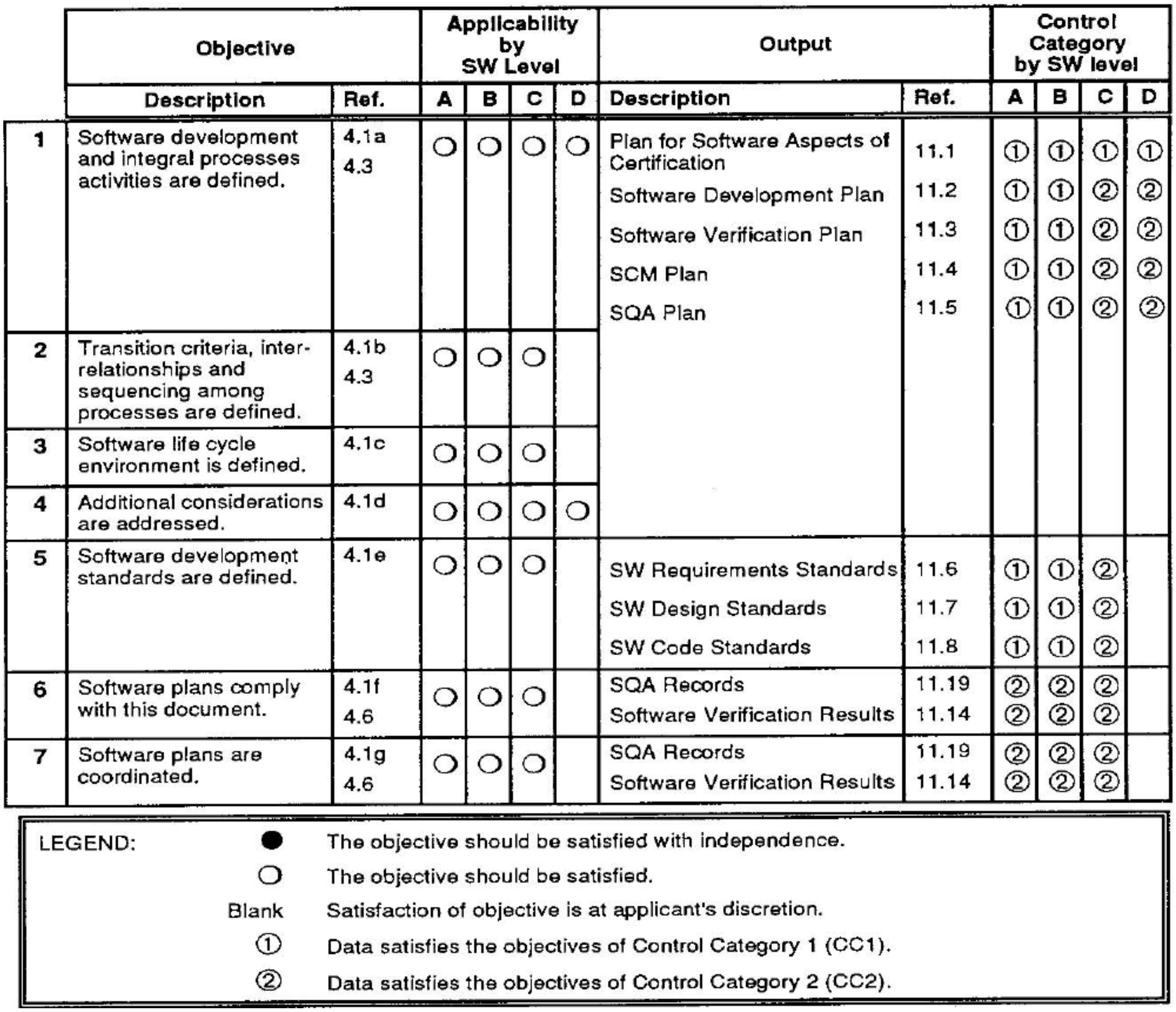
Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
7.0 Process Assurance Process														
7.1	Assurance is obtained that necessary plans are developed and maintained for all aspects of system certification.	5.7.3	R*	R*	R*	R	N	Evidence of Process Assurance	②	②	②	②		
7.2	Development activities and processes are conducted in accordance with those plans.	5.7.4	R*	R*	R*	R	N	Evidence of Process Assurance	②	②	②	②		
R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification. * Independence is achieved when the process assurance activity is performed by a person(s) other than the developer.														

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
8.0 Certification and Regulatory Authority Coordination Process														
8.1	Compliance substantiation is provided.	5.8.3	R	R	R	A	N	Certification Summary	①	①	①	②		
		5.8.4.2	R	R	R	A	N	Configuration Index	①	①	②	②		
R*- Recommended for certification with process independence, R - Recommended for certification, A - As negotiated for certification, N - Not required for certification.														

APPENDIX B: DO-178B PROCESS OBJECTIVES DATA AND CONTROL CATEGORIES[24]

[24] Excerpted from: Software Considerations in Airborne Systems and Equipment Certification, Radio Technical Commission on Aeronautics, Document 178 Revision B

Software Planning Process

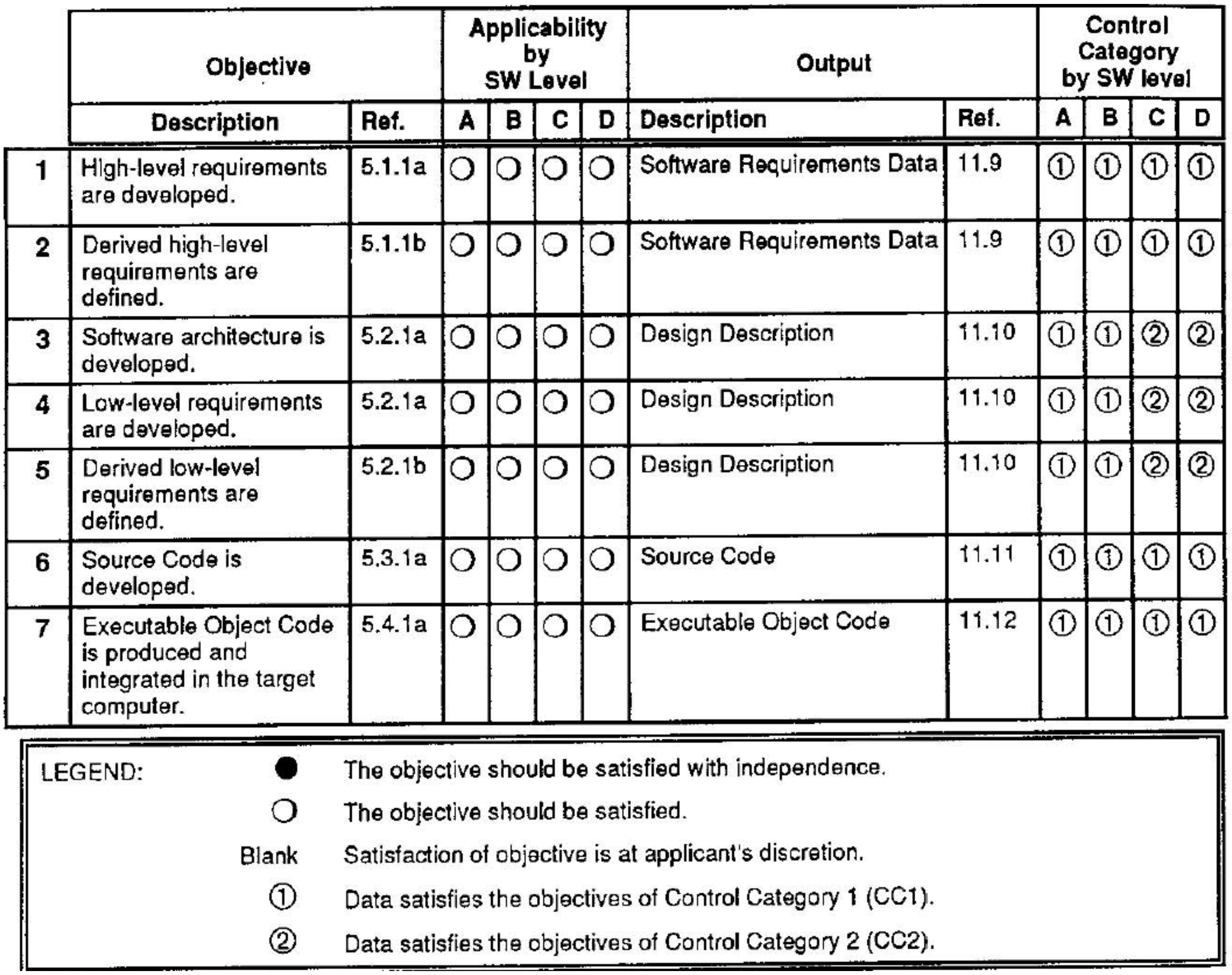


	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Software development and integral processes activities are defined.	4.1a 4.3	○	○	○	○	Plan for Software Aspects of Certification Software Development Plan Software Verification Plan SCM Plan SQA Plan	11.1 11.2 11.3 11.4 11.5	① ① ① ① ①	① ① ① ① ①	① ② ② ② ②	① ② ② ② ②
2	Transition criteria, inter-relationships and sequencing among processes are defined.	4.1b 4.3	○	○	○							
3	Software life cycle environment is defined.	4.1c	○	○	○							
4	Additional considerations are addressed.	4.1d	○	○	○	○						
5	Software development standards are defined.	4.1e	○	○	○		SW Requirements Standards SW Design Standards SW Code Standards	11.6 11.7 11.8	① ① ①	① ① ①	② ② ②	
6	Software plans comply with this document.	4.1f 4.6	○	○	○		SQA Records Software Verification Results	11.19 11.14	② ②	② ②	② ②	
7	Software plans are coordinated.	4.1g 4.6	○	○	○		SQA Records Software Verification Results	11.19 11.14	② ②	② ②	② ②	

LEGEND:

●	The objective should be satisfied with independence.
○	The objective should be satisfied.
Blank	Satisfaction of objective is at applicant's discretion.
①	Data satisfies the objectives of Control Category 1 (CC1).
②	Data satisfies the objectives of Control Category 2 (CC2).

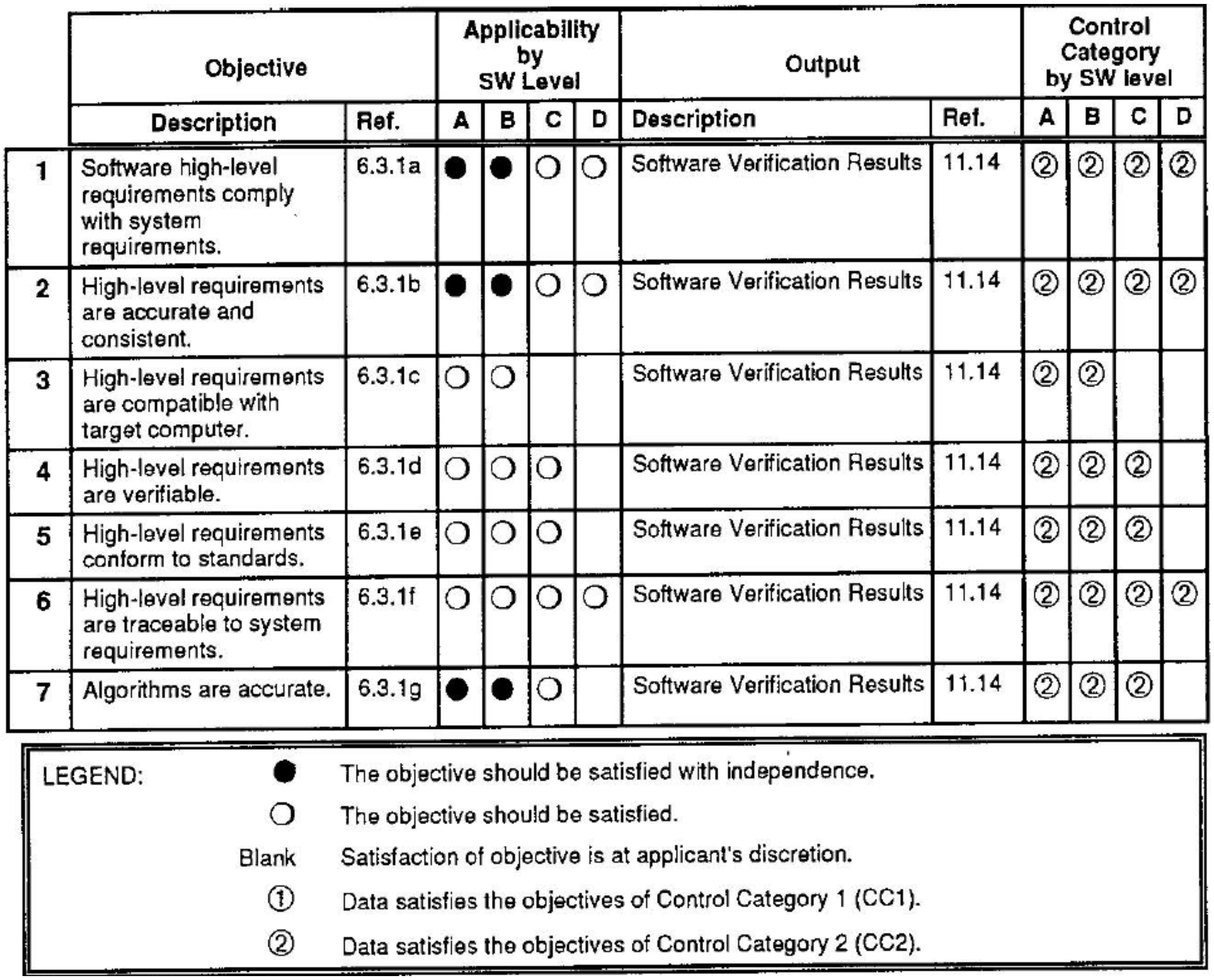
Software Development Processes



	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	High-level requirements are developed.	5.1.1a	○	○	○	○	Software Requirements Data	11.9	①	①	①	①
2	Derived high-level requirements are defined.	5.1.1b	○	○	○	○	Software Requirements Data	11.9	①	①	①	①
3	Software architecture is developed.	5.2.1a	○	○	○	○	Design Description	11.10	①	①	②	②
4	Low-level requirements are developed.	5.2.1a	○	○	○	○	Design Description	11.10	①	①	②	②
5	Derived low-level requirements are defined.	5.2.1b	○	○	○	○	Design Description	11.10	①	①	②	②
6	Source Code is developed.	5.3.1a	○	○	○	○	Source Code	11.11	①	①	①	①
7	Executable Object Code is produced and integrated in the target computer.	5.4.1a	○	○	○	○	Executable Object Code	11.12	①	①	①	①

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Verification of Outputs of Software Requirements Process

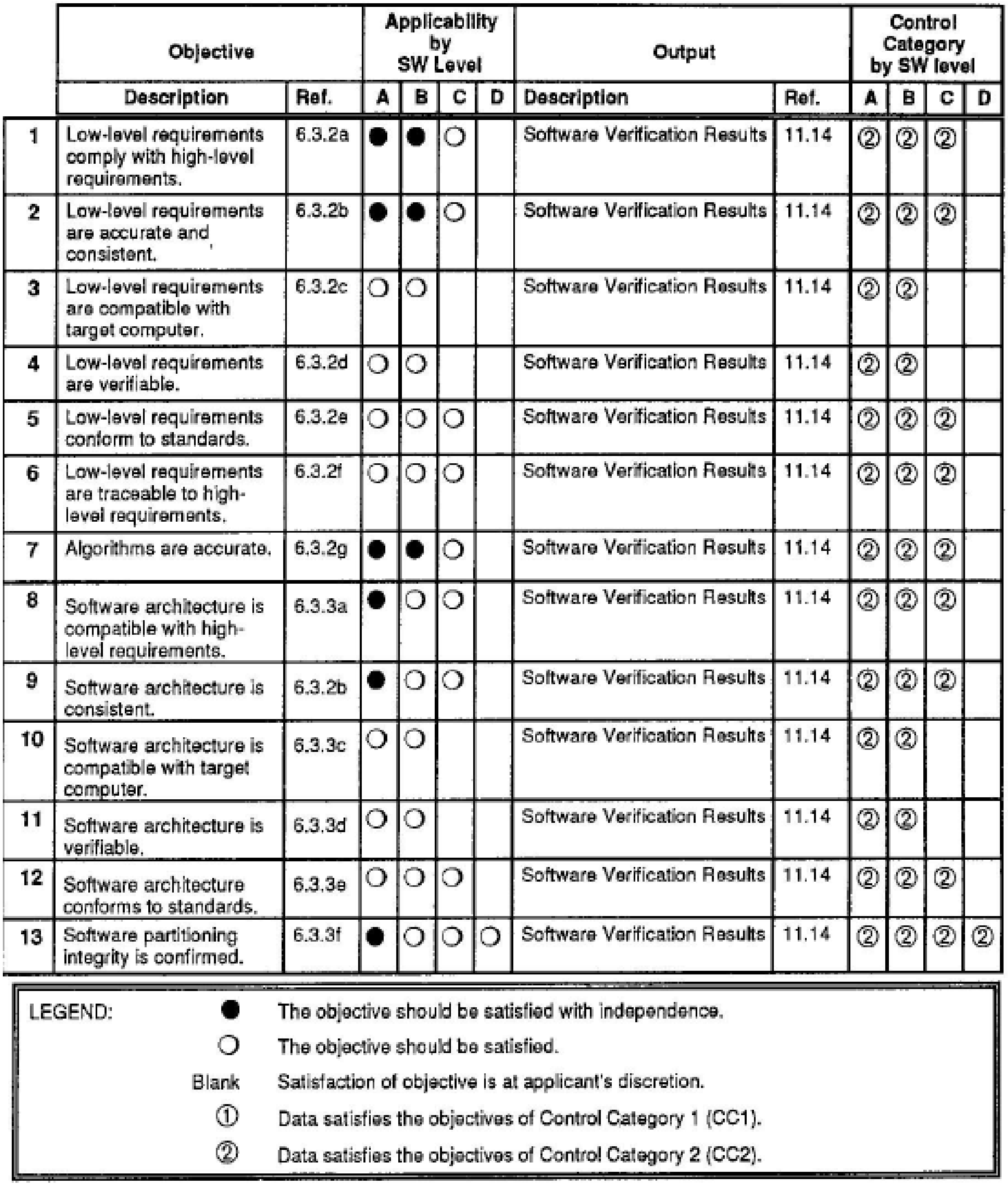


	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Software high-level requirements comply with system requirements.	6.3.1a	●	●	○	○	Software Verification Results	11.14	②	②	②	②
2	High-level requirements are accurate and consistent.	6.3.1b	●	●	○	○	Software Verification Results	11.14	②	②	②	②
3	High-level requirements are compatible with target computer.	6.3.1c	○	○			Software Verification Results	11.14	②	②		
4	High-level requirements are verifiable.	6.3.1d	○	○	○		Software Verification Results	11.14	②	②	②	
5	High-level requirements conform to standards.	6.3.1e	○	○	○		Software Verification Results	11.14	②	②	②	
6	High-level requirements are traceable to system requirements.	6.3.1f	○	○	○	○	Software Verification Results	11.14	②	②	②	②
7	Algorithms are accurate.	6.3.1g	●	●	○		Software Verification Results	11.14	②	②	②	

LEGEND:

LEGEND:	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

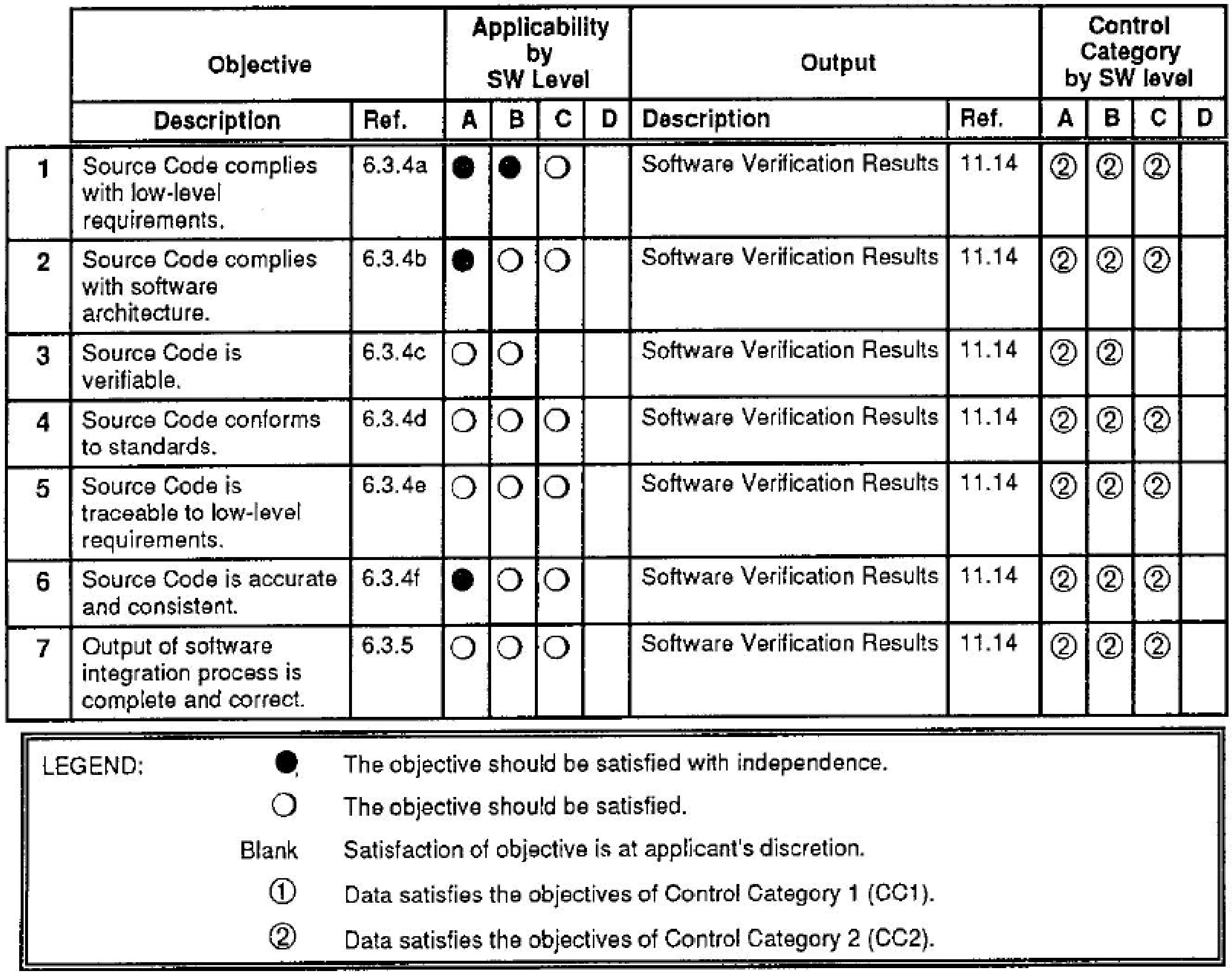
Verification of Outputs of Software Design Process



	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Low-level requirements comply with high-level requirements.	6.3.2a	●	●	○		Software Verification Results	11.14	②	②	②	
2	Low-level requirements are accurate and consistent.	6.3.2b	●	●	○		Software Verification Results	11.14	②	②	②	
3	Low-level requirements are compatible with target computer.	6.3.2c	○	○			Software Verification Results	11.14	②	②		
4	Low-level requirements are verifiable.	6.3.2d	○	○			Software Verification Results	11.14	②	②		
5	Low-level requirements conform to standards.	6.3.2e	○	○	○		Software Verification Results	11.14	②	②	②	
6	Low-level requirements are traceable to high-level requirements.	6.3.2f	○	○	○		Software Verification Results	11.14	②	②	②	
7	Algorithms are accurate.	6.3.2g	●	●	○		Software Verification Results	11.14	②	②	②	
8	Software architecture is compatible with high-level requirements.	6.3.3a	●	○	○		Software Verification Results	11.14	②	②	②	
9	Software architecture is consistent.	6.3.2b	●	○	○		Software Verification Results	11.14	②	②	②	
10	Software architecture is compatible with target computer.	6.3.3c	○	○			Software Verification Results	11.14	②	②		
11	Software architecture is verifiable.	6.3.3d	○	○			Software Verification Results	11.14	②	②		
12	Software architecture conforms to standards.	6.3.3e	○	○	○		Software Verification Results	11.14	②	②	②	
13	Software partitioning integrity is confirmed.	6.3.3f	●	○	○	○	Software Verification Results	11.14	②	②	②	②

LEGEND:	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

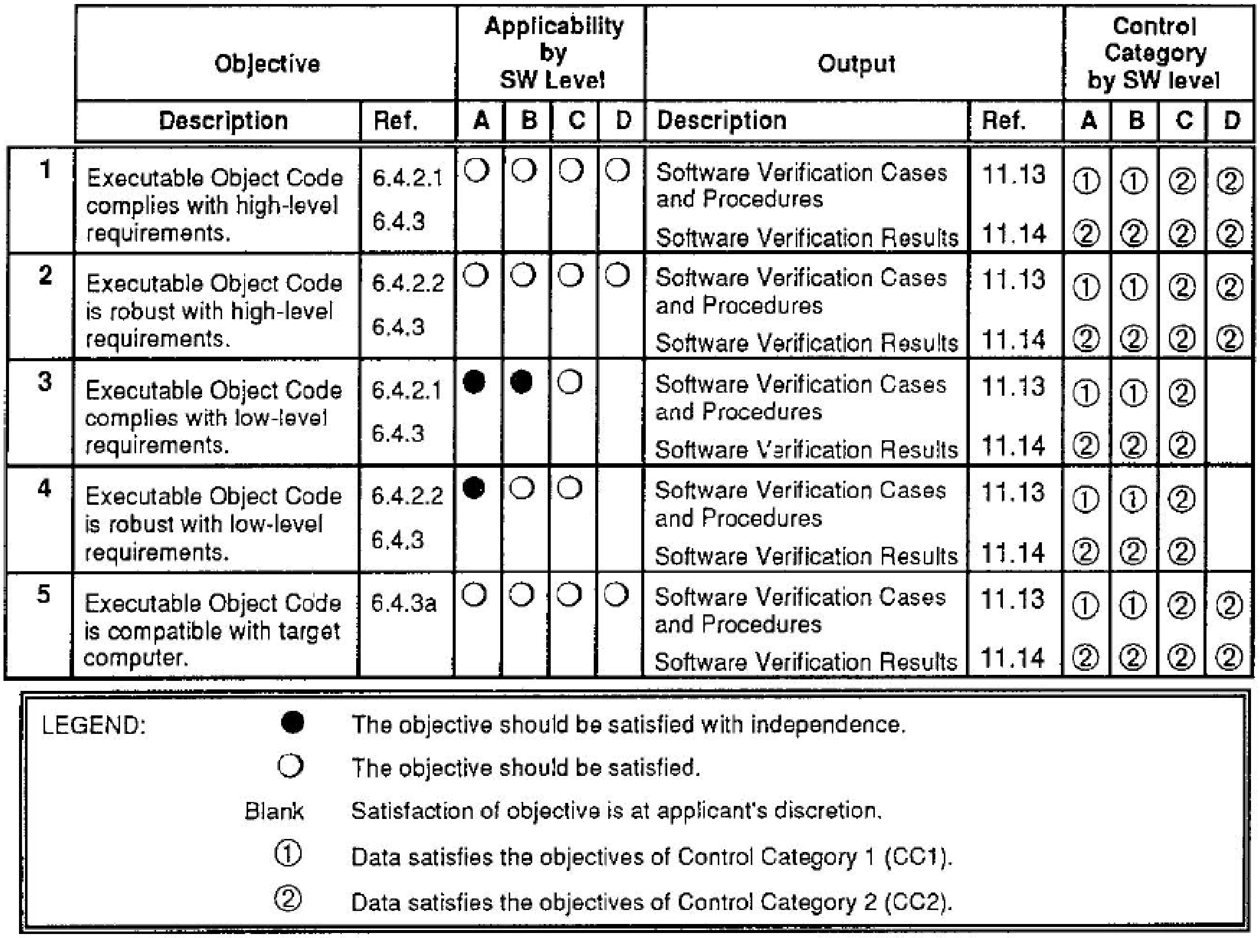
Verification of Outputs of Software Coding & Integration Processes



	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Source Code complies with low-level requirements.	6.3.4a	●	●	○		Software Verification Results	11.14	②	②	②	
2	Source Code complies with software architecture.	6.3.4b	●	○	○		Software Verification Results	11.14	②	②	②	
3	Source Code is verifiable.	6.3.4c	○	○			Software Verification Results	11.14	②	②		
4	Source Code conforms to standards.	6.3.4d	○	○	○		Software Verification Results	11.14	②	②	②	
5	Source Code is traceable to low-level requirements.	6.3.4e	○	○	○		Software Verification Results	11.14	②	②	②	
6	Source Code is accurate and consistent.	6.3.4f	●	○	○		Software Verification Results	11.14	②	②	②	
7	Output of software integration process is complete and correct.	6.3.5	○	○	○		Software Verification Results	11.14	②	②	②	

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

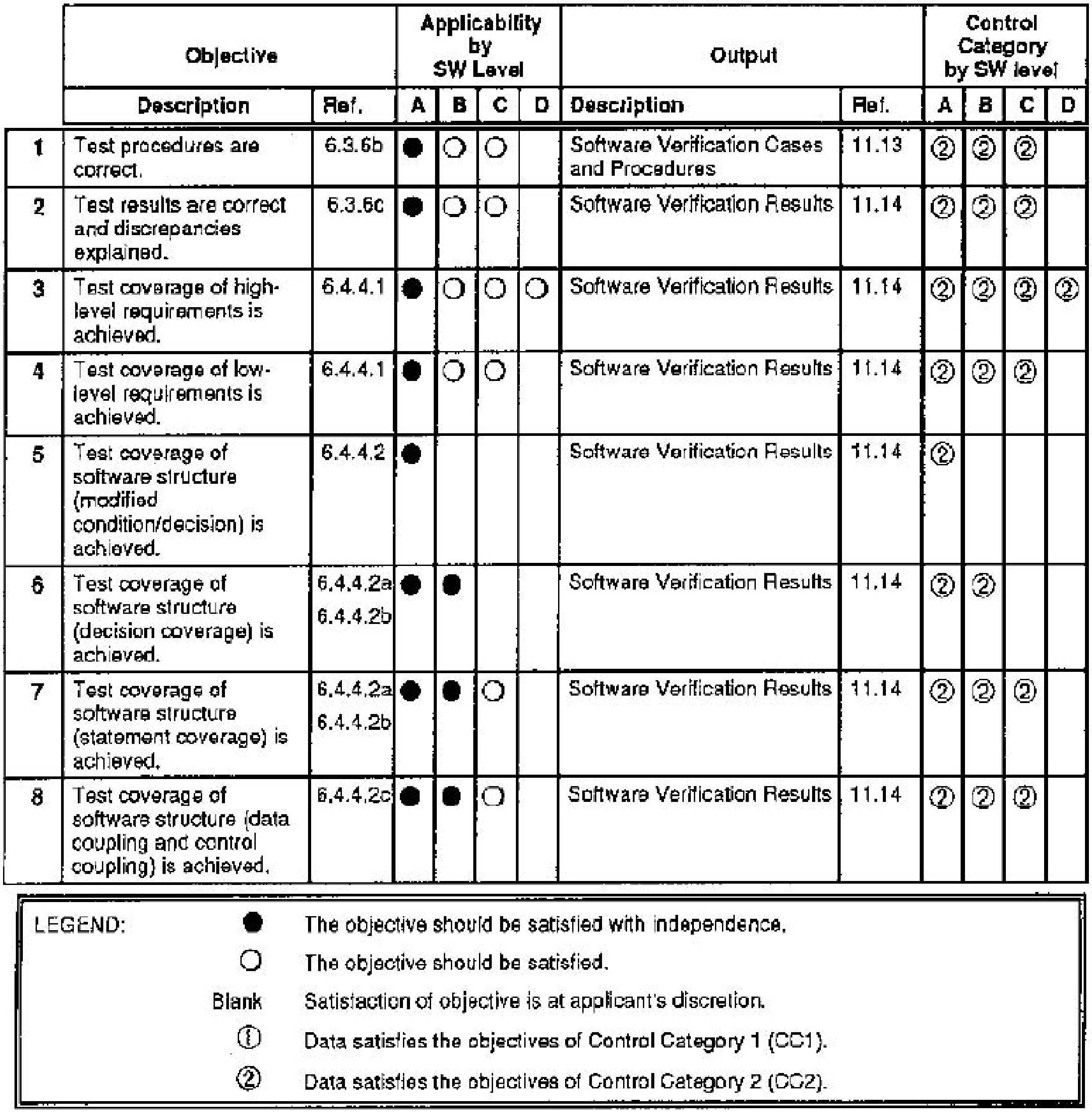
Testing of Outputs of Integration Process



	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Executable Object Code complies with high-level requirements.	6.4.2.1 6.4.3	○	○	○	○	Software Verification Cases and Procedures Software Verification Results	11.13 11.14	① ②	① ②	② ②	② ②
2	Executable Object Code is robust with high-level requirements.	6.4.2.2 6.4.3	○	○	○	○	Software Verification Cases and Procedures Software Verification Results	11.13 11.14	① ②	① ②	② ②	② ②
3	Executable Object Code complies with low-level requirements.	6.4.2.1 6.4.3	●	●	○		Software Verification Cases and Procedures Software Verification Results	11.13 11.14	① ②	① ②	② ②	
4	Executable Object Code is robust with low-level requirements.	6.4.2.2 6.4.3	●	○	○		Software Verification Cases and Procedures Software Verification Results	11.13 11.14	① ②	① ②	② ②	
5	Executable Object Code is compatible with target computer.	6.4.3a	○	○	○	○	Software Verification Cases and Procedures Software Verification Results	11.13 11.14	① ②	① ②	② ②	② ②

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Verification of Verification Process Results

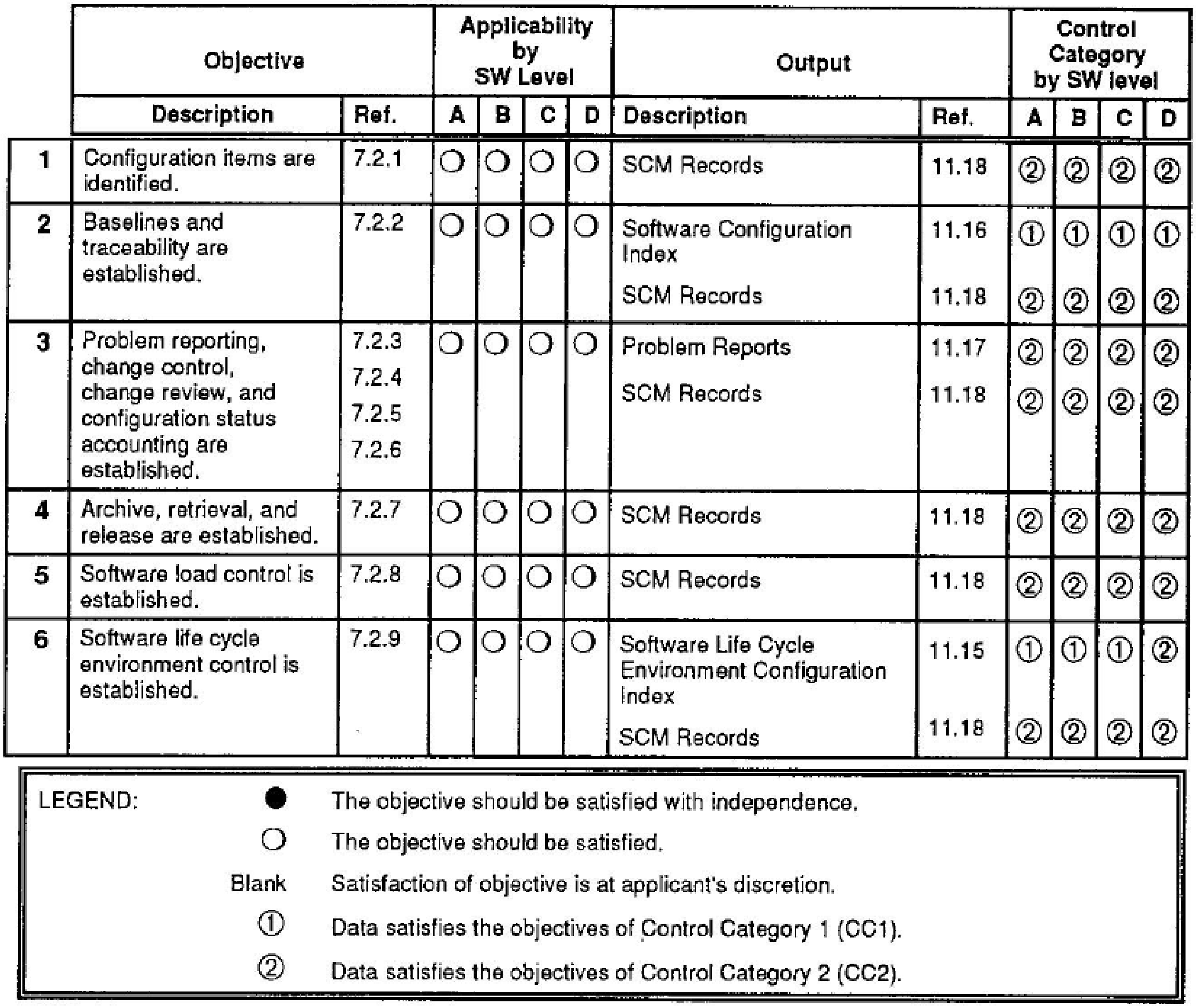


	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Test procedures are correct.	6.3.6b	●	○	○		Software Verification Cases and Procedures	11.13	②	②	②	
2	Test results are correct and discrepancies explained.	6.3.6c	●	○	○		Software Verification Results	11.14	②	②	②	
3	Test coverage of high-level requirements is achieved.	6.4.4.1	●	○	○	○	Software Verification Results	11.14	②	②	②	②
4	Test coverage of low-level requirements is achieved.	6.4.4.1	●	○	○		Software Verification Results	11.14	②	②	②	
5	Test coverage of software structure (modified condition/decision) is achieved.	6.4.4.2	●				Software Verification Results	11.14	②			
6	Test coverage of software structure (decision coverage) is achieved.	6.4.4.2a 6.4.4.2b	●	●			Software Verification Results	11.14	②	②		
7	Test coverage of software structure (statement coverage) is achieved.	6.4.4.2a 6.4.4.2b	●	●	○		Software Verification Results	11.14	②	②	②	
8	Test coverage of software structure (data coupling and control coupling) is achieved.	6.4.4.2c	●	●	○		Software Verification Results	11.14	②	②	②	

LEGEND:

LEGEND:	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

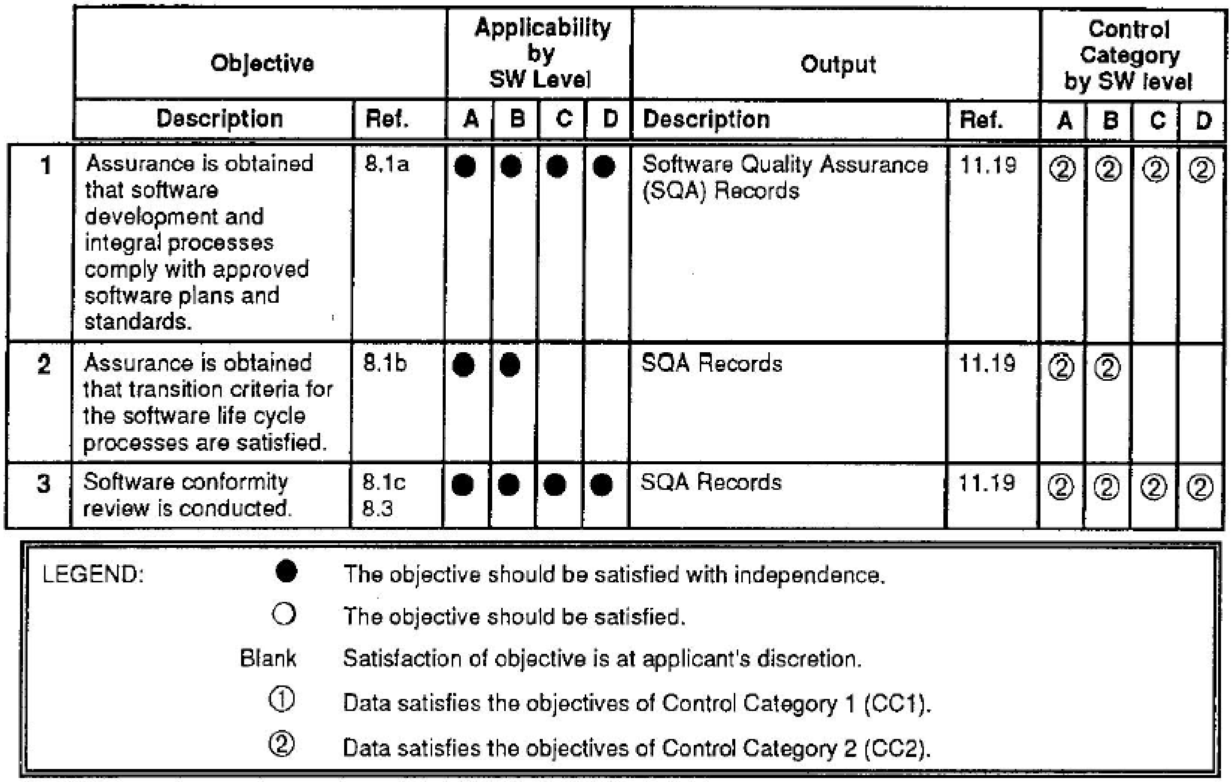
Software Configuration Management Process



	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Configuration items are identified.	7.2.1	○	○	○	○	SCM Records	11.18	②	②	②	②
2	Baselines and traceability are established.	7.2.2	○	○	○	○	Software Configuration Index	11.16	①	①	①	①
							SCM Records	11.18	②	②	②	②
3	Problem reporting, change control, change review, and configuration status accounting are established.	7.2.3 7.2.4 7.2.5 7.2.6	○	○	○	○	Problem Reports	11.17	②	②	②	②
							SCM Records	11.18	②	②	②	②
4	Archive, retrieval, and release are established.	7.2.7	○	○	○	○	SCM Records	11.18	②	②	②	②
5	Software load control is established.	7.2.8	○	○	○	○	SCM Records	11.18	②	②	②	②
6	Software life cycle environment control is established.	7.2.9	○	○	○	○	Software Life Cycle Environment Configuration Index	11.15	①	①	①	②
							SCM Records	11.18	②	②	②	②

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Software Quality Assurance Process



	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Assurance is obtained that software development and integral processes comply with approved software plans and standards.	8.1a	●	●	●	●	Software Quality Assurance (SQA) Records	11.19	②	②	②	②
2	Assurance is obtained that transition criteria for the software life cycle processes are satisfied.	8.1b	●	●			SQA Records	11.19	②	②		
3	Software conformity review is conducted.	8.1c 8.3	●	●	●	●	SQA Records	11.19	②	②	②	②

LEGEND:

● The objective should be satisfied with independence.

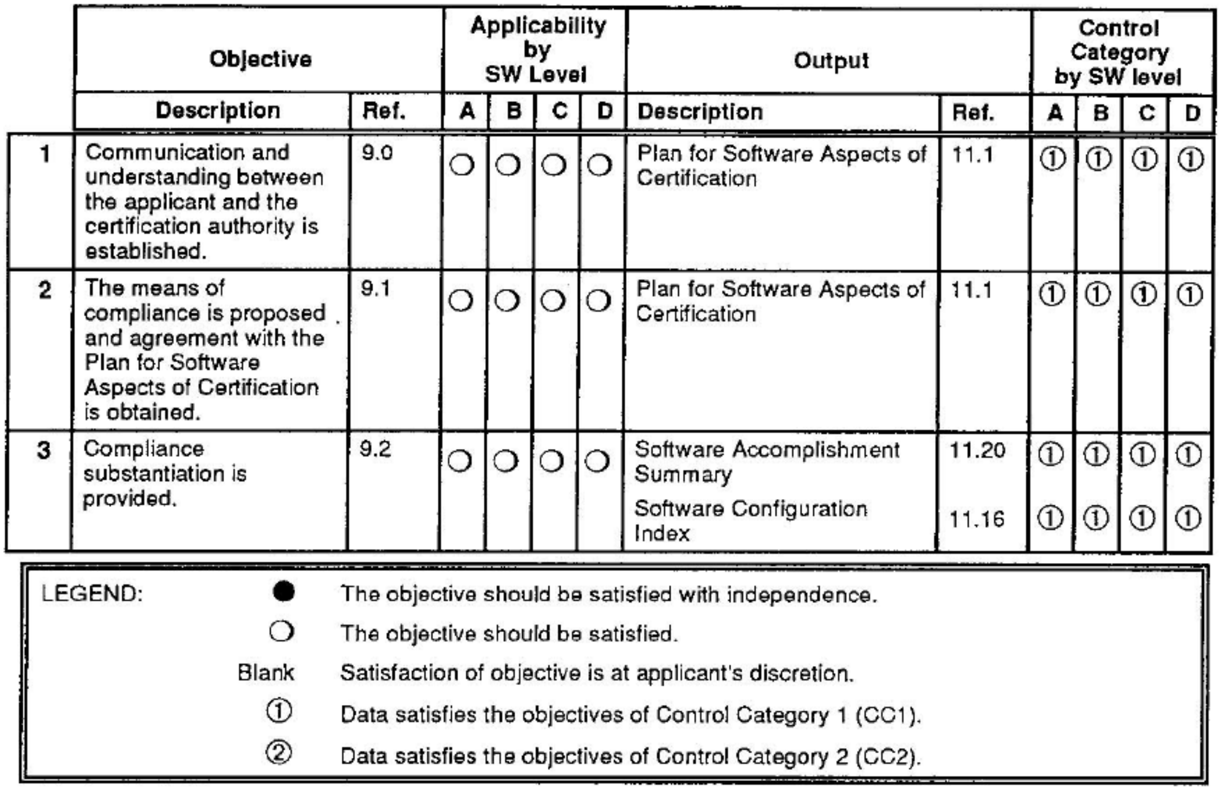
○ The objective should be satisfied.

Blank Satisfaction of objective is at applicant's discretion.

① Data satisfies the objectives of Control Category 1 (CC1).

② Data satisfies the objectives of Control Category 2 (CC2).

Certification Liaison Process



	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Communication and understanding between the applicant and the certification authority is established.	9.0	○	○	○	○	Plan for Software Aspects of Certification	11.1	①	①	①	①
2	The means of compliance is proposed and agreement with the Plan for Software Aspects of Certification is obtained.	9.1	○	○	○	○	Plan for Software Aspects of Certification	11.1	①	①	①	①
3	Compliance substantiation is provided.	9.2	○	○	○	○	Software Accomplishment Summary Software Configuration Index	11.20 11.16	① ①	① ①	① ①	① ①

LEGEND:		
	●	The objective should be satisfied with independence.
	○	The objective should be satisfied.
	Blank	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

APPENDIX C: DO-254 HARDWARE LIFE CYCLE DATA AND HARDWARE CONTROL CATEGORIES[25]

[25] Excerpted from: Design Assurance Guidance for Airborne Electronic Hardware, Radio Technical Commission on Aeronautics, Document 254

Data Section	Hardware Life Cycle Data ①	Objectives ②	Submit	Level A	Level B	Level C	Level D
10.1	Hardware Plans						
10.1.1	Plan for Hardware Aspects of Certification	4.1(1,2,3,4)	S	HC1	HC1	HC1	HC1
10.1.2	Hardware Design Plan	4.1(1,2,3,4)		HC2	HC2	HC2	NA
10.1.3	Hardware Validation Plan ③④	4.1(1,2,3,4); 6.1.1(1)		HC2	HC2	HC2	NA
10.1.4	Hardware Verification Plan	4.1(1,2,3,4); 6.2.1(1)	S	HC2	HC2	HC2	HC2
10.1.5	Hardware Configuration Management Plan	4.1(1,2,3,4); 7.1(3)		HC1	HC1	HC2	HC2
10.1.6	Hardware Process Assurance Plan	4.1(1,2,4); 8.1(1,2,3)		HC2	HC2	NA	NA
10.2	Hardware Design Standards						
10.2.1	Requirements Standards ③	4.1(2)		HC2	HC2	NA	NA
10.2.2	Hardware Design Standards ③	4.1(2)		HC2	HC2	NA	NA
10.2.3	Validation and Verification Standards ③	4.1(2)		HC2	HC2	NA	NA
10.2.4	Hardware Archive Standards ③	4.1(2);5.5.1(1); 7.1(1,2)		HC2	HC2	NA	NA

Data Section	Hardware Life Cycle Data ①	Objectives ②	Submit	Level A	Level B	Level C	Level D
10.3	Hardware Design Data						
10.3.1	Hardware Requirements	5.1.1(1,2); 5.2.1(2); 5.3.1(2); 5.4.1(3); 5.5.1(1,2,3); 6.1.1(1,2); 6.2.1(1)		HC1	HC1	HC1	HC1
10.3.2	Hardware Design Representation Data						
10.3.2.1	Conceptual Design Data ③	5.2.1(1)		HC2	HC2	NA	NA
10.3.2.2	Detailed Design Data	5.3.1(1); 5.4.1(2)		⑤	⑤	⑤	⑤
10.3.2.2.1	Top-Level Drawing	5.3.1(1); 5.4.1(2); 5.5.1(1)	S	HC1	HC1	HC1	HC1
10.3.2.2.2	Assembly Drawings	5.3.1(1); 5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.3	Installation Control Drawings	5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.4	Hardware/Software Interface Data ③	5.3.1(1); 5.5.1(1)		HC1	HC1	HC1	HC1

Data Section	Hardware Life Cycle Data ①	Objectives ②	Submit	Level A	Level B	Level C	Level D
10.4	Validation And Verification Data						
10.4.1	Hardware Traceability Data	6.1.1(1); 6.2.1(1,2)		HC2	HC2	HC2 ⑥	HC2 ⑥
10.4.2	Hardware Review and Analysis Procedures ③	6.1.1(1,2); 6.2.1(1)		HC1	HC1	NA	NA
10.4.3	Hardware Review and Analysis Results ③	6.1.1(1,2); 6.2.1(1)		HC2	HC2	HC2	HC2
10.4.4	Hardware Test Procedures ③	6.1.1(1,2); 6.2.1(1)		HC1	HC1	HC2	HC2 ⑦
10.4.5	Hardware Test Results ③	6.1.1(1,2); 6.2.1(1)		HC2	HC2	HC2	HC2 ⑦
10.5	Hardware Acceptance Test Criteria	5.5.1(3),6.2.1(3)		HC2	HC2	HC2	HC2
10.6	Problem Reports	5.1.1(3); 5.2.1(3); 5.3.1(3); 5.4.1(4); 5.5.1(4); 6.1.1(3); 6.2.1(4); 7.1(3)		HC2	HC2	HC2	HC2
10.7	Hardware Configuration Management Records	5.5.1(1); 7.1(1,2,3)		HC2	HC2	HC2	HC2
10.8	Hardware Process Assurance Records	7.1(2); 8.1(1,2,3)		HC2	HC2	HC2	NA
10.9	Hardware Accomplishment Summary	8.1(1,2,3)	S	HC1	HC1	HC1	HC1

① Data that should be submitted is indicated by an S in the Submit column. HC1 and HC2 data used for certification that need not be submitted should be available. Refer to Section 7.3.

② The objectives listed here are for reference only. Not all objectives may be applicable to all assurance levels.

③ If this data is used for certification, then its availability is shown in the table. This data is not always used for certification and may not be required.

④ This can be accomplished informally through the certification liaison process for Levels C and D. Documentation can be in the form of meeting minutes and or presentation material.

⑤ If the applicant references this data item in submitted data items, it should be available.

⑥ Only the traceability data from requirements to test is needed.

⑦ Test coverage of derived or lower hierarchical requirements is not needed.