

# WOLF CREEK

NUCLEAR OPERATING CORPORATION

Terry J. Garrett  
Vice President, Engineering

September 20, 2007

ET 07-0041

U. S. Nuclear Regulatory Commission  
ATTN: Document Control Desk  
Washington, DC 20555

- Reference:
- 1) Letter ET 07-0004, dated March 14, 2007, from T. J. Garrett, WCNOG, to USNRC
  - 2) Letter ET 07-0022, dated June 15, 2007, from T. J. Garrett, WCNOG, to USNRC
  - 3) Letter dated August 8, 2007, from J. W. Lubinski, USNRC, to R. A. Muench, WCNOG
  - 4) Letter ET 07-0039, dated August 31, 2007, from T. J. Garrett, WCNOG, to USNRC

Subject: Docket No. 50-482: Additional Response to NRC Letter dated August 8, 2007, Regarding the Main Steam and Feedwater Isolation System Controls Modification

Gentlemen:

Reference 1 provided a license amendment request that proposed revisions to Technical Specification (TS) 3.3.2, "Engineered Safety Feature Actuation System (ESFAS) Instrumentation," TS 3.7.2, "Main Steam Isolation Valves (MSIVs)," and TS 3.7.3, "Main Feedwater Isolation Valves (MFIVs)." Reference 1 proposed changes to these specifications based on a planned modification to replace the MSIVs and associated actuators, MFIVs and associated actuators, and replacement of the Main Steam and Feedwater Isolation System (MSFIS) controls. On August 2, 2007, Wolf Creek Nuclear Operating Corporation (WCNOG) personnel met with the Nuclear Regulatory Commission (NRC) to discuss five issues identified by the NRC staff associated with the review of the MSFIS controls modification. Subsequently, Reference 3 provided the results of the meeting and requested WCNOG to respond to the five issues. As discussed at the August 2, 2007 meeting, and documented in Reference 3, the first issue was to provide by September 20, 2007, a detailed mapping of RTCA DO-254/EUROCAE ED 80, "Design Assurance Guidance for Airborne Electronic Hardware," to Institute of Electrical

A001  
NRC

and Electronics Engineers (IEEE) Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." The Attachment provides WCNO's response to issue 1.

Reference 2 provided supplemental information on the MSFIS controls modification. In the response to item 22, WCNO made a commitment that the Operations and Maintenance Manual would be developed by September 14, 2007 with acceptance of the manual by September 28, 2007. A review of information and schedules associated with this commitment determined that WCNO had provided an incorrect date for completing the Operations and Maintenance Manual. The correct date for completion of the manual is November 30, 2007 with WCNO acceptance of the manual by December 14, 2007. This information was provided to the NRC Project Manager by electronic mail on September 14, 2007.

The additional information provided in the Attachment and Enclosure do not impact the conclusions of the No Significant Hazards Consideration provided in Reference 1. In accordance with 10 CFR 50.91, a copy of this submittal (without the Enclosure) is being provided to the designated Kansas State official.

Attachment II provides a list of commitments made in this letter. If you have any questions concerning this matter, please contact me at (620) 364-4084, or Mr. Kevin Moles at (620) 364-4126.

Sincerely,



Terry J. Garrett

TJG/rlt

Attachments I) Response to NRC Letter Regarding the Main Steam and Feedwater Isolation System (MSFIS) Controls Modification  
II) List of Commitments

Enclosure

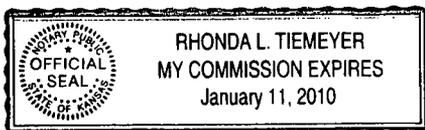
cc: E. E. Collins (NRC), w/a, w/e  
T. A. Conley (KDHE), w/a,  
J. N. Donohew (NRC), w/a, w/e  
V. G. Gaddy (NRC), w/a, w/e  
Senior Resident Inspector (NRC), w/a, w/e

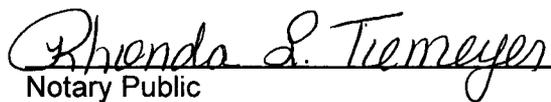
STATE OF KANSAS    )  
                                  ) SS  
COUNTY OF COFFEY )

Terry J. Garrett, of lawful age, being first duly sworn upon oath says that he is Vice President Engineering of Wolf Creek Nuclear Operating Corporation; that he has read the foregoing document and knows the contents thereof; that he has executed the same for and on behalf of said Corporation with full power and authority to do so; and that the facts therein stated are true and correct to the best of his knowledge, information and belief.

By   
Terry J. Garrett  
Vice President Engineering

SUBSCRIBED and sworn to before me this 20<sup>th</sup> day of Sept., 2007.



  
Notary Public

Expiration Date January 11, 2010

## **Response to NRC Letter Regarding the Main Steam and Feedwater Isolation System (MSFIS) Controls Modification**

On August 2, 2007, Wolf Creek Nuclear Operating Corporation (WCNOC) personnel met with the Nuclear Regulatory Commission (NRC) staff to discuss five issues identified by the NRC associated with the review of the MSFIS controls modification. Subsequently, the NRC issued a letter dated August 8, 2007, in which the NRC staff accepted the MSFIS controls modification license amendment request for review. This letter identified 5 issues requiring a response from WCNOC. WCNOC letter ET 07-0039, dated August 31, 2007, provided responses to the 5 issues. With regard to issue 1, WCNOC indicated that a more detailed comparison of RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware," to Institute of Electrical and Electronics Engineers (IEEE) Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," would be provided by September 20, 2007. Issue 1 and supplemental response is provided below.

*1. The standard which the licensee chose to use to develop this system, RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware," has not been reviewed or approved for nuclear safety-related use at nuclear power plants by the NRC staff. At this point, the licensee should provide a detailed mapping of this standard to an NRC-approved standard such as the Institute of Electrical and Electronic Engineers (IEEE) Standard 7-4.3.2, and show on a paragraph-by-paragraph basis what portion of standard RTCA DO-254/EUROCAE ED-80 has similar requirements, and why meeting that portion of RTCA DO-254/EUROCAE ED-80 will satisfy the corresponding section of the approved IEEE standard. There may be sections of the approved standard which are not applicable to an FPGA design, and these should be pointed out and justified. The NRC staff should receive the results of this task by September 20, 2007, as the licensee agreed to in the August 2, 2007, meeting. If this date is not met or the quality of the information is not sufficient, our acceptance of the review of the proposed replacement MSFIS will be retracted.*

**Response:** WCNOC contracted with HighRely, Inc. to perform a difference analysis between RTCA DO-254 and IEEE 7-4.3.2. WCNOC chose HighRely to perform this analysis based on their familiarity and experience with DO-254 and knowledge of IEEE 7-4.3.2. The IEEE 7-4.3.2 – DO-254 Difference Analysis is provided in Enclosure I. WCNOC has indicated in letter ET 07-0039 that the MSFIS controls is a software-based digital system from the standpoint that there is high quality software utilized in the Field Programmable Gate Array (FPGA) logic development process and therefore, will meet the applicable criteria of IEEE 7-4.3.2-2003. WCNOC is available for a meeting with the technical branch reviewer the week of October 15 to discuss Enclosure I, if necessary. We believe that a meeting would be beneficial in explaining the difference analysis and the applicability of IEEE 7-4.3.2 to the WCGS design.

The difference analysis performed by HighRely, Inc. has identified several key aspects of the relationship between the aviation industry and nuclear industry standards for complex digital systems. The difference analysis was specifically scoped to compare IEEE 7-4.3.2 and DO-254, however during the analysis there were several interviews with the HighRely engineers, and it became apparent that this is not an easy comparison to make. The expectation had initially been a paragraph-by-paragraph comparison, but once the details of the analysis began to formulate, WCNOC realized this would not be possible. Given this difficulty of the paragraph-by-paragraph comparison, a written comparison was made to highlight the differences between the two standards.

The difference analysis identifies the fact that IEEE 7-4.3.2 is more heavily focused on the system level while DO-254 is focused on the low level steps of the development process. As the analysis progresses it becomes further apparent that IEEE 7-4.3.2 and DO-254 have many similarities but are basically at a different level within the overall set of standards for the respective industries, Aviation and Nuclear. In other words, DO-254 relies on system level aspects being provided by standards above it, such as SAE ARP 4754, "Certification Consideration for Highly-Integrated or Complex Aircraft Systems," and SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment." This is similar in the way that IEEE 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," provides higher-level aspects, which drive down to IEEE 7-4.3.2.

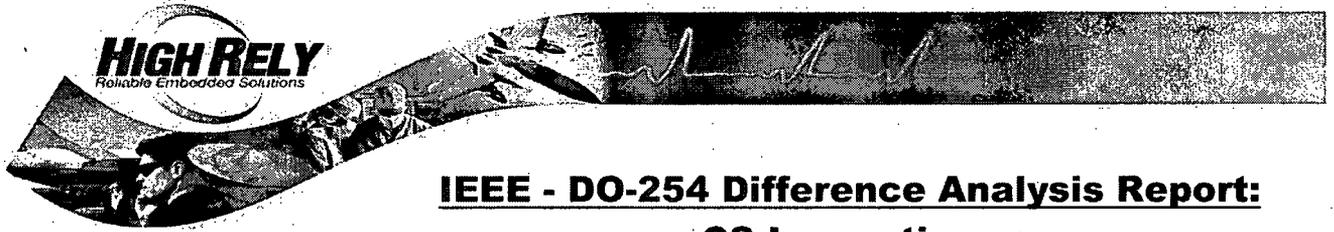
WCNOC believes that DO-254 provides useful design guidance for complex digital electronics, particularly since the standard is focused on Programmable Logic Devices (PLDs), Application Specific Integrated Circuits (ASICs), and FPGAs based designs. However, WCNOC does not believe that DO-254 is a substitute for IEEE 7-4.3.2, rather; it is a complement to IEEE 7-4.3.2. WCNOC concludes that IEEE 7-4.3.2 is an appropriate standard for complex digital electronics particularly since the focus of this standard is at the system level. WCNOC does not discourage the use of DO-254 as design guidance since the DO-254 standard contains many aspects that compliment IEEE 7-4.3.2. As indicated in letter ET 07-0039, the MSFIS controls will meet the applicable criteria of IEEE 7-4.3.2-2003.

### LIST OF COMMITMENTS

The following table identifies those actions committed to by Wolf Creek Nuclear Operating Corporation in this document. Any other statements in this letter are provided for information purposes and are not considered regulatory commitments. Please direct questions regarding these commitments to Mr. Kevin Moles, Manager Regulatory Affairs at Wolf Creek Generating Station, (620) 364-4126.

REGULATORY COMMITMENT	DUE DATE
The Operations and Maintenance Manual will be developed by November 30, 2007 with acceptance of the manual by December 14, 2007	11/30/2007 12/14/2007

**IEEE 7-4.3.2 – DO-254 Difference Analysis**

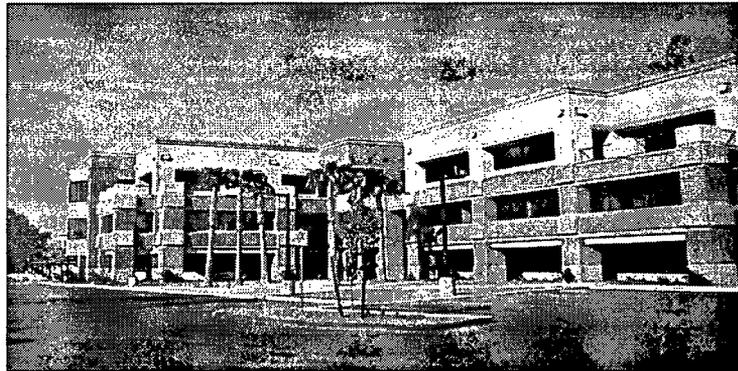


**IEEE - DO-254 Difference Analysis Report:**  
**CS Innovations**

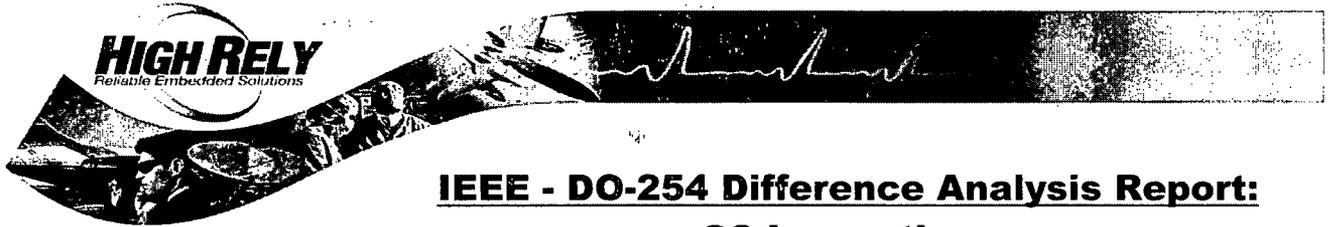
**IEEE 7-4.3.2 - DO-254 Difference Analysis**

*CS Innovations*

August 22, 2007



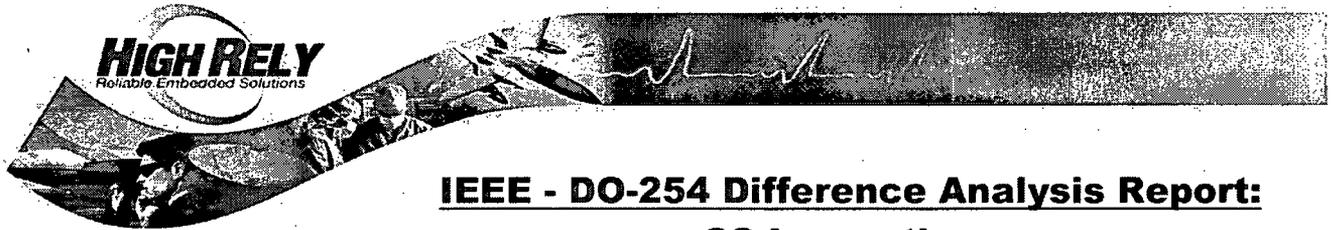
***HighRely Avionics & Certification Center  
Phoenix, Arizona***



## **IEEE - DO-254 Difference Analysis Report:** **CS Innovations**

### **Table of Contents**

1	DO-254 Difference Analysis Overview .....	3
1.1	DO-254 Summary.....	4
2	Summary: IEEE 7-4.3.2 to DO-254 Analysis.....	11
2.1	Summary of IEEE 7-4.3.2 and DO-254 Differences .....	12
2.2	Summary of IEEE 7-4.3.2 and DO-254.....	19
2.3	Conclusions .....	19
3	Complex Electronic Hardware (CEH) Difference Analysis .....	21
3.1	Hardware (ASIC/PLD) Planning Process .....	21
3.2	Hardware (ASIC/PLD) Architectural Decisions .....	23
3.3	Hardware (ASIC/PLD) Requirements Capture .....	29
3.4	Hardware (ASIC/PLD) Preliminary Design (behavioral, Conceptual design) .....	31
3.5	Hardware (ASIC/PLD) Detailed Design (synthesis, mask generation, fuse file) .....	32
3.6	Hardware (ASIC/PLD) Fabrication (programming programmable components/Implementation) .....	33
3.7	Hardware (ASIC/PLD) Production Transition .....	35
3.8	Hardware (ASIC/PLD) Validation and Verification (timing analysis, behavioral simulation, gate level simulation and design).....	37
3.9	Hardware (ASIC/PLD) Configuration Management Process .....	40
3.10	Hardware (ASIC/PLD) Process Assurance .....	42
3.11	Hardware (ASIC/PLD) Certification Liaison Process .....	44
3.12	Hardware (ASIC/PLD) Additional Consideration for Levels A&B .....	45
4	IEEE 7-4.3.2 Deliverables and Aviation Process Equivalent .....	45
4.1	DO-254 Deliverables are defined as:.....	46
4.2	Deliverables of IEEE 7-4.3.2 Vs. Aviation Standards .....	50



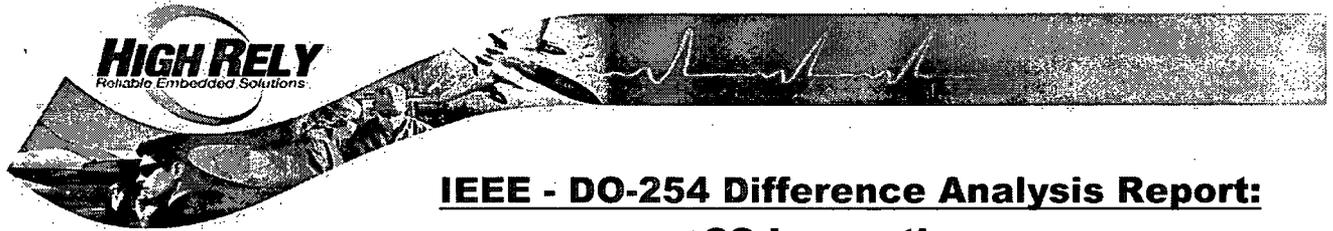
## **IEEE - DO-254 Difference Analysis Report:** **CS Innovations**

### **1 DO-254 Difference Analysis Overview**

CS Innovations has requested HighRely Incorporated to perform a Difference Analysis between RTCA DO-254/ED-80, Design Assurance Guidance for Airborne Electronic Hardware (DO-254) and IEEE Std 7-4.3.2 – 2003™ IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (IEEE 7-4.3.2). The purpose of this Difference Analysis is to identify the differences, gap and/or shortcomings pertinent to the complex electronic hardware development under the guidance of DO-254 as compared with those identified in IEEE 7-4.3.2. Specifically, HighRely's Difference Analysis provides for the following activities crucial to DO-254 compliance and certification:

- 1. Assessment of IEEE 7-4.3.2 and the engineering approach contained therein.*
- 2. Detailed analysis and cross-reference of the IEEE approach as it pertains to DO-254.*
- 3. Explanation of differences using HighRely's DO-254 Analysis Checklist; Section 3 of this Report.*
- 4. Onsite explanation by HighRely of key DO-254 aspects, common risks and risk-mitigation techniques.*
- 5. High-level findings of DO-254 differences and comments regarding these differences.*

CS Innovations has a history of developing complete electronics systems, specializing in hardware and system development, with expert designers in embedded system architecture, integrated circuits, analog, digital and software. While this exercise does not directly assess them in any detail, CS Innovations' engineering disciplines appear to be well established. Included in these disciplines are configuration management, quality assurance and engineering and manufacturing activities and capabilities that are well suited for safety system development. This assessment is made based on interviews with both CS Innovations and Wolf Creek Generating Station personnel.



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

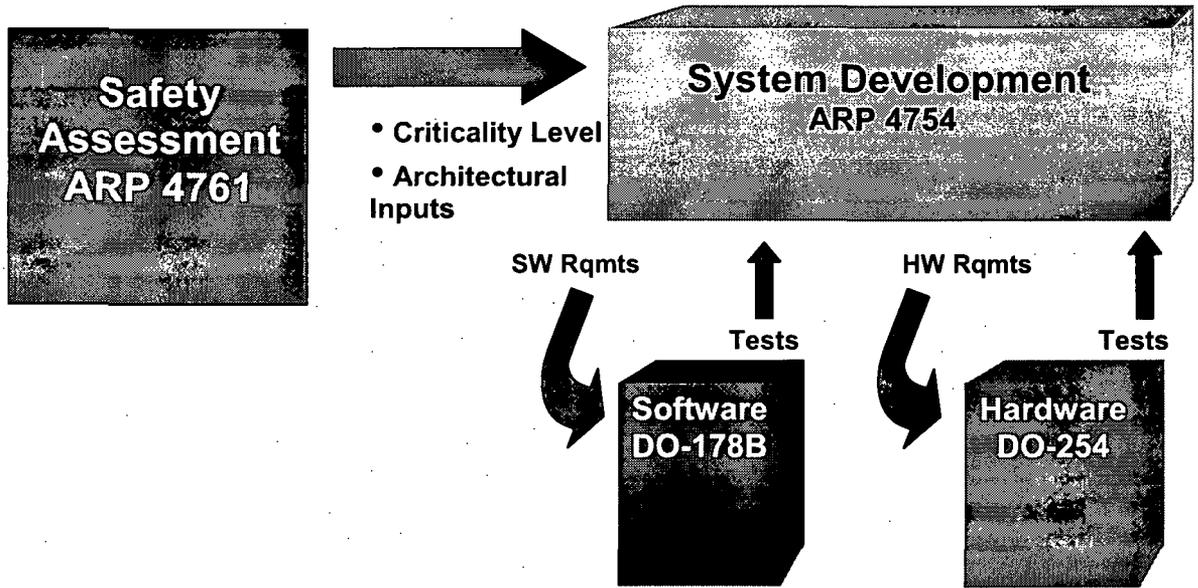
### **1.1 DO-254 Summary**

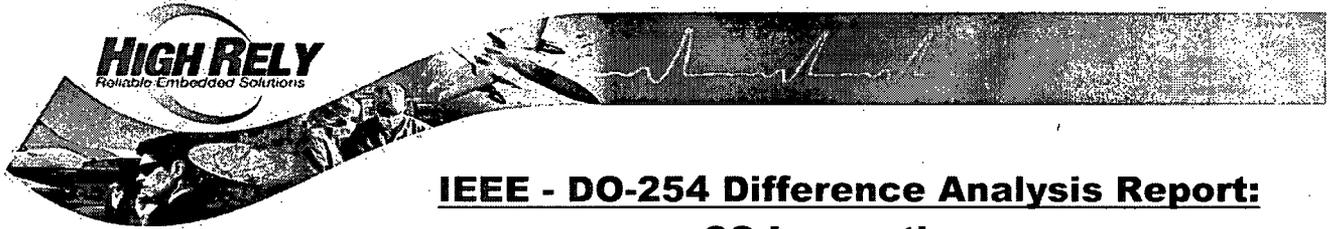
The DO-254 document provides guidance for design assurance of airborne electronic hardware from conception through initial certification and subsequent post certification product improvements to ensure continued airworthiness. DO-254 was released in April 2000 and its intent is to provide developmental assurance for complex electronic hardware including programmable logic devices (PLDs) and application specific integrated circuits (ASICs) and other decision making hardware devices. Following the guidance and procedures outlined in DO-254 assures that the hardware design performs its intended functions in its specified environment, and meets airworthiness requirements. DO-254 does not specify design considerations for system development, but does discuss a relationship to the system development process; which includes the overlapping, iterative feedback nature of system and component development processes, as well as the exchange of information between the system development process and the complex electronic hardware design lifecycle process. As well, DO-254 does not specify the considerations for the software development process, but indicates an exchange of information between the processes.

RTCA/DO-254 distinguishes between complex and simple electronic hardware; recognizes five levels of failure effects ranging from catastrophic to no affect; and provides guidance for each hardware design assurance level. Although the guidance in RTCA/DO-254 is applicable to all categories of hardware items (e.g., Line Replaceable Units (LRUs), Circuit Board Assemblies, etc) guidance is provided for custom micro-coded components (e.g., ASICs, PLDs, and FPGAs).

The following figures depict the scope, contents, and application of DO-254. A subsequent table lists the primary themes of DO-254; all of these DO-254 aspects are evaluated for this project and covered in this difference analysis. Each of these DO-254 Themes is separately assessed and differences analyzed. Recommendations for further study are presented. A table of IEEE 7-4.3.2 outputs as compared to aviation deliverables is also provided.

**Figure 1-1: DO-254/DO-178B Overview - Safety, System, Software & Hardware**

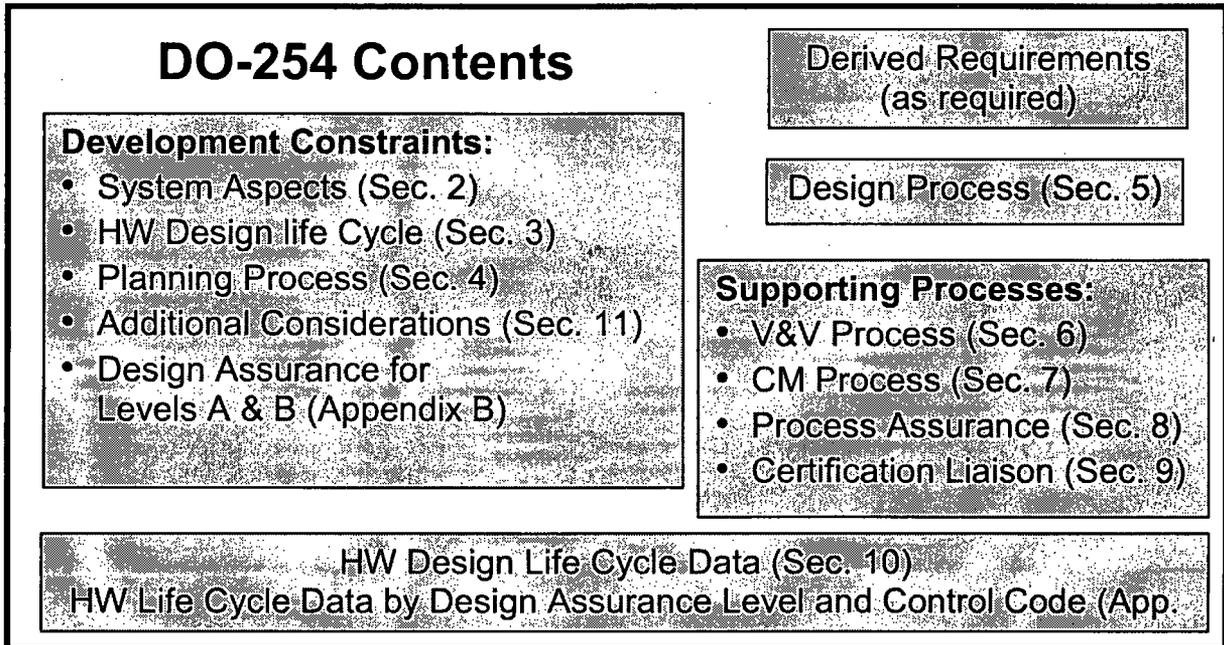


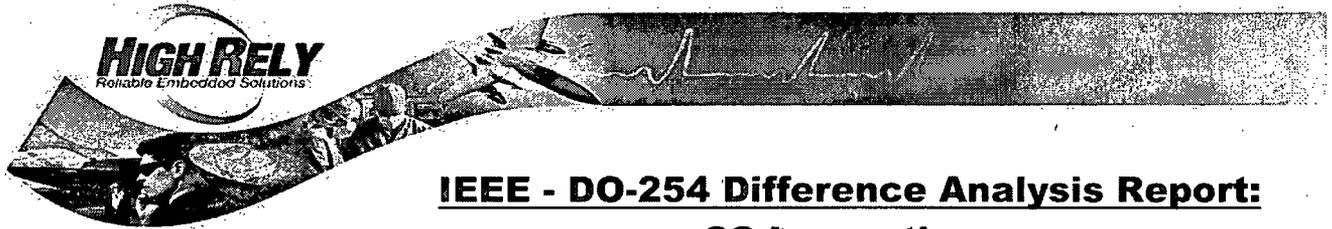


## **IEEE - DO-254 Difference Analysis Report:**

### **CS Innovations**

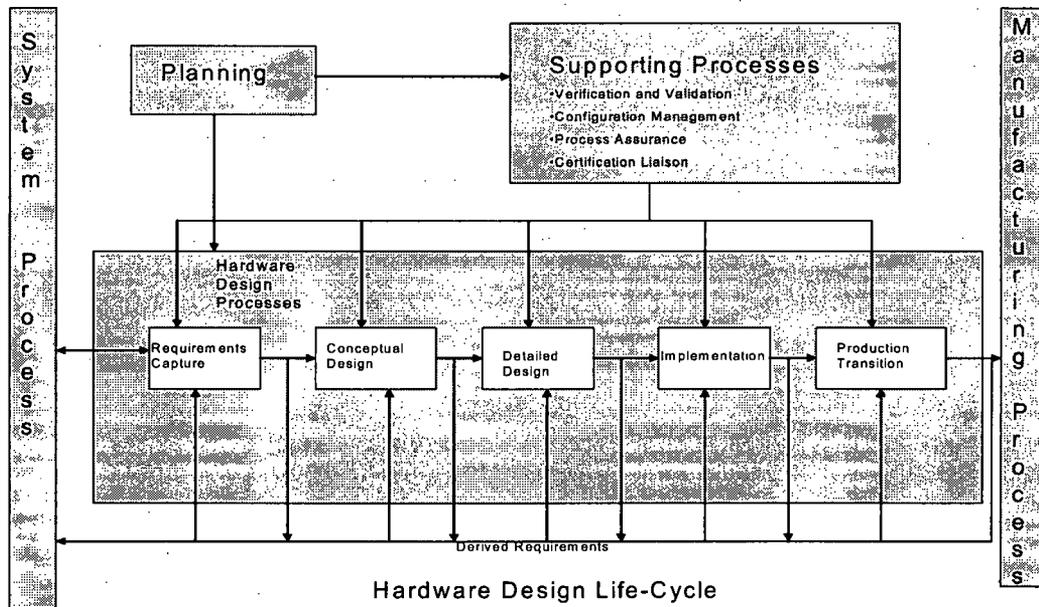
**Figure 1-2: DO-254 Document Contents Overview**

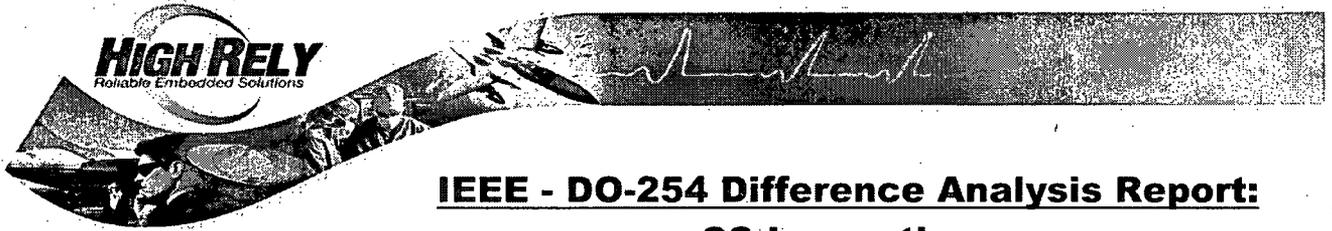




## IEEE - DO-254 Difference Analysis Report: CS Innovations

**Figure 1-3: DO-254 Hardware Development Lifecycle Overview**

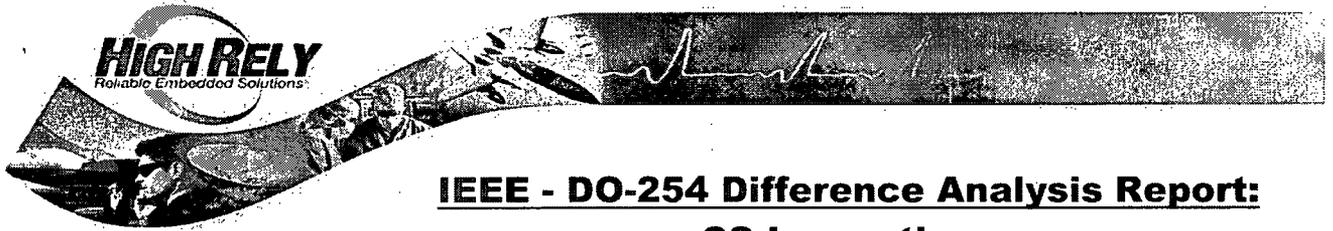




## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

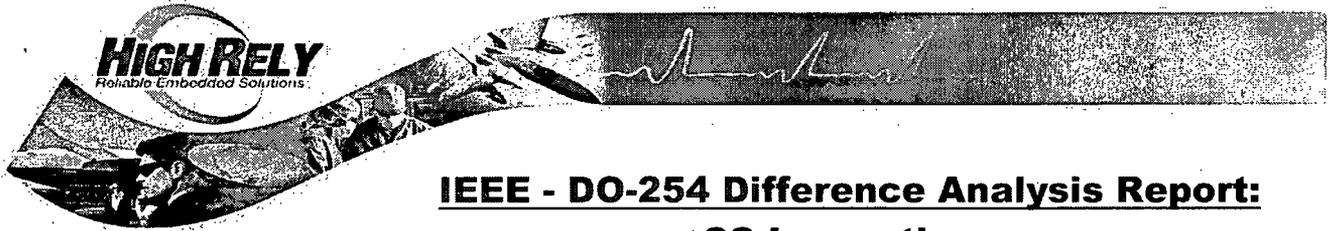
The following table lists the Top Ten common themes of DO-254; all of these DO-254 aspects are evaluated and covered in HighRelY's Difference Analysis as presented herein. Each of these DO-254 themes is separately addressed relative to IEEE 7-4.3.2 and separately described herein, complete with HighRelY commentary and recommendations.

<b>DO-254 Theme</b>	<b>General High-Level Description</b>
<b>Safety Assessment Process</b>	There are three system safety assessment processes: functional hazard assessment (FHA), preliminary system safety assessment (PSSA) and SSA. These processes are used to establish the system safety objectives applicable to the system development assurance process, and to determine that the system functions achieve certifiable safety objectives.
<b>Hardware Planning Process</b>	The purpose of the hardware planning process is to define the means by which the functional and airworthiness requirements are converted into a hardware item with an acceptable amount of evidence of assurance that the item will safely perform its intended functions. The objectives of the hardware planning process are: the design life-cycle processes are defined, standards are selected and defined, development and verification are selected and defined, and the means of compliance including strategies for safety are proposed and conveyed.
<b>System &amp; Hardware Architecture Planning &amp; Development</b>	Given the safety, functional and performance requirements allocated to the hardware by the system process, the hardware safety assessment determines the hardware design assurance level for each function and contributes to determining the appropriate design assurance strategies to be used. Architectural design decisions take into account the system safety, functional and performance requirements.
<b>Hardware Requirements</b>	The requirements capture process identifies and records the hardware item requirements. This includes those derived requirements imposed by the proposed hardware item architecture, choice of technology, the basic and optional functionality, environmental, and performance requirements as well as the requirements imposed by the system safety assessment.



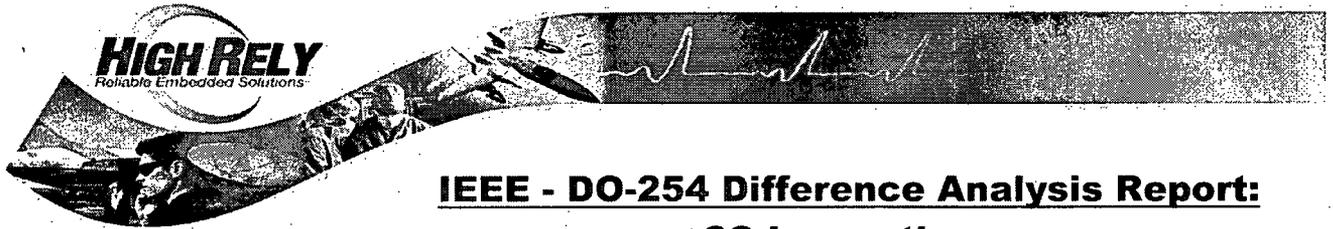
**IEEE - DO-254 Difference Analysis Report:**  
**CS Innovations**

<i>DO-254 Theme</i>	<i>General High-Level Description</i>
<b>Hardware Conceptual Design</b>	The conceptual design process produces a high-Level Design concept that may be assessed to determine the potential for the resulting design implementation to meet the requirements. This may be accomplished using such items as functional block diagrams, design and architecture descriptions, circuit card assembly outlines, and chassis sketches.
<b>Hardware Detailed Design</b>	The detailed design process produces detailed design data using the hardware item requirements and conceptual design data as the basis for the detailed design.
<b>Hardware Implementation &amp; Production Transition</b>	The implementation process uses the detailed design data to produce the hardware item that is an input to the testing activity. In this process, manufacturing data, test facilities and general resources should be examined to ensure availability and suitability for production. The production transition process uses the outputs from the implementation and verification processes to move the product into production.
<b>Hardware Verification &amp; Validation</b>	The validation process provides assurances that the hardware item derived requirements are correct and complete with respect to system requirements allocated to the hardware item. The verification process provides assurance that the hardware item implementation meets all of the hardware requirements, including derived requirements.
<b>Hardware Configuration Management</b>	The configuration management process is intended to provide the ability to consistently replicate the configuration item, regenerate the information if necessary and modify the configuration item in a controlled fashion if modification is necessary.
<b>Hardware Process Assurance</b>	Process assurance ensures that the life cycle process objectives are met and activities have been completed as outlined in plans or that deviations have been addressed. Unlike software, DO-254 production assurance extends through manufacturing, as building the hardware is equally important to designing it.



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

<b>DO-254 Theme</b>	<b>General High-Level Description</b>
Hardware Certification Liaison	The purpose of the certification liaison process is to establish communication and understanding between the applicant and the certification authority throughout the hardware design life cycle to assist in the certification process. Liaison activities may include design approach presentation for timely approval, negotiations concerning the means of compliance with the certification basis, approval of design approach, means of data approval, and any required certification authority reviews and witnessing of tests. For DO-254, Liaison is performed via DER with a Systems ticket augmented with DO-254 certification.



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

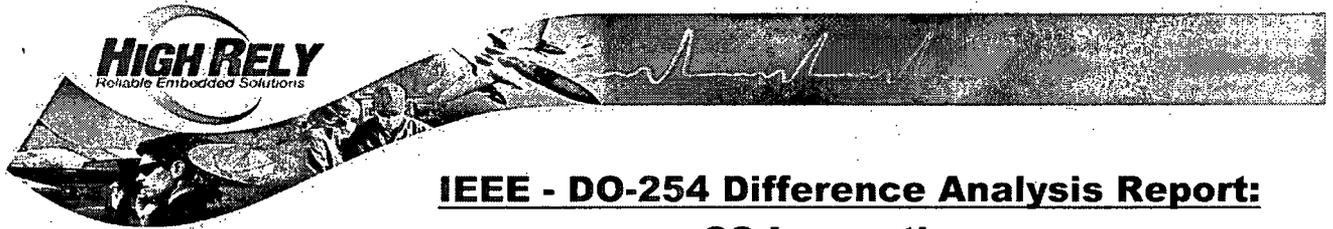
### **2 Summary: IEEE 7-4.3.2 to DO-254 Analysis**

This section presents a summary of IEEE 7-4.3.2 and DO-254 similarities and differences and related issues for Complex Electronic Hardware (CEH). As previously mentioned, HighRely's DO-254 Difference Analysis provides an independent, detailed, and accurate assessment of DO-254 related activities in comparison to those stated in IEEE 7-4.3.2, along with recommendations for filling any gaps between the standards. The scope of this report is limited to IEEE 7-4.3.2. IEEE 7-4.3.2 makes reference to multiple IEEE standards, the details of which are considered out of the scope of this analysis, however those additional standards parallel the primary IEEE standard compared herein.

In essence, IEEE 7-4.3.2 and DO-254 have many similarities, with both aiming to improve the measurable quality, repeatability, and auditability of critical complex electronic systems. Many characteristics reflect a typical computer system development process, including conceptual design, requirements development, implementation, requirements-based testing, acceptance testing, production and operation. For these characteristics, IEEE 7-4.3.2 points to IEEE 603-1998 along with other IEEE standards and a comparison between these standards and DO-254 is not within scope of this exercise. IEEE 7-4.3.2 does, however, necessitate requirements necessary to meet the quality criterion of safety systems. These include software development, qualification of COTS, use of software tools, verification and validation, configuration management and risk management. DO-254 also addresses these aspects, but in a fashion where the details are embedded within the design assurance guidance for the appropriate criticality level.

In order to accommodate different cost structures based on the intended use of a system or subsystem, DO-254 provides a unique means for varying criticality levels based on system functionality as integrated into an airborne platform; determined via various safety assessments and hazard analyses integrated into formal system requirements. DO-254 also allows for protection through partitioning of systems and subsystems based on the intended use and safety assessment. Since IEEE 7-4.3.2 is specifically targeted to nuclear power generating stations, this report focuses on DO-254 design assurance for criticality Level A; that is the criticality at the highest level defined, and does not detail aspects of lower criticality levels as described in DO-254.

IEEE 7-4.3.2 is focused more heavily upon system development aspects versus the development lifecycle and low-level steps inherent in DO-254. As an example, Annex E of IEEE 7-4.3.2 discusses communication independence in great detail. It is apparent that the discussion in Annex E is appropriate to the development of data communication between a single safety channel, between safety channels and between safety and non-safety computer systems; and the possibility of the loss of a computer's ability to perform its function. This discussion leads to the development of appropriate system level requirements; but does not provide assurance that the refinement of those requirements, the allocation of those requirements, the specification of an adequate complex electronic hardware design, the implementation of that design, and that the verification that the requirements were implemented correctly is accomplished. The development using DO-254 of communication independent system designs, such as those presented in Annex E, would provide for assurances that the system is specified, designed and implemented completely and correctly.



## **IEEE - DO-254 Difference Analysis Report:** **CS Innovations**

Similar to the explanation above regarding Annex E, IEEE 7-4.3.2 presents a section discussing system integrity. This discussion is intended to ensure that the system is designed for integrity, designed for test and calibration and designed for fault detection and self-diagnosis. While presented in a different context, this system integrity parallels DO-254's precursor safety assessment process, whereby the architecture is refined to support the desired safety (criticality) level. When these design considerations are adequately specified (outside the scope of DO-254), developing the system under the guidance of DO-254 will ensure that the system performs its intended function without introducing error and that no unintended function is inadvertently introduced during the development lifecycle.

*It is intended that the reader fully review and absorb the detailed findings as contained in the sections herein; those sections contain the complete HighRelY DO-254 Difference Analysis and DO-254 Checklists along with discrete nuances of individual findings.*

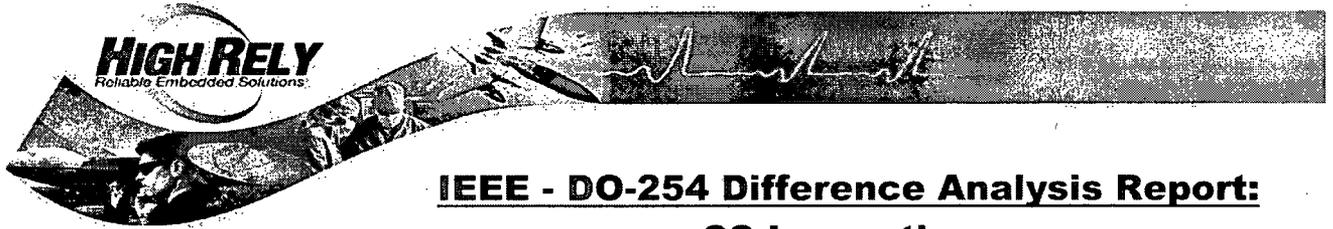
### **2.1 Summary of IEEE 7-4.3.2 and DO-254 Differences**

IEEE 7-4.3.2 discusses safety systems in general, and delves into the specific aspects of Nuclear Power Generating Stations, but does not directly address the safety system design basis; rather defers to IEEE Std 603-1998. DO-254, refers to SAE ARP 4754 as a source of development guidance for highly integrated or complex systems and SAE ARP 4761 as a source of safety assessment methods to be used in the hardware design assurance process. While these processes may be similar or equivalent, this report does not make that assessment official as it is beyond the scope, however it is the authors' opinions that these process have similar goals and similar implementation practices including hazard assessment, functional hazard assessments, failure modes effect analysis, and safety assessments.

DO-254 also refers to RTCA DO-178/EUROCAE ED-12 for Software Considerations in Airborne Systems and Equipment Certification as well as RTCA DO-160/ EUROCAE ED-14 for Environmental Conditions and Test Procedures for Airborne Equipment. The current version of DO-178 is DO-178B and the current version of DO-160 is DO-160E. The three, DO-254, DO-178B and DO-160E, combined provide for the overall design assurance of airborne equipment. This report does not assess the considerations or conditions described in DO-178B or DO-160E.

IEEE 7-4.3.2 discusses safety system criteria in terms of the quality of the development, equipment qualification, system integrity, independence and identification; whereas DO-254 discusses design assurance for various levels of criticality with an emphasis on process and objective evidence. The quality, independence, integrity and identification considerations are embedded in the lifecycle processes discussed in DO-254.

Both software and hardware are discussed within IEEE 7-4.3.2 (and IEEE Std 603-1998, and IEEE/EIA Std 12207.0-1996), where DO-254 focuses on complex electronic hardware. Complex electronic hardware is loosely defined as hardware that is capable of producing varying results based on decision making aspects contained within the hardware device. A significant difference between IEEE 7-4.3.2 and DO-254 is the use of the term 'firmware'. IEEE 7-4.3.2 attempts to define firmware as a combination of a hardware device and computer instructions and data that reside as read-only software on that device. In



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

essence, IEEE 7-4.3.2 defines firmware as non-loadable software. IEEE 7-4.3.2 also briefly discusses allocating functional and performance requirements to hardware and software (Section C.2.2), but does not discuss allocation to firmware.

DO-254 does not attempt to define firmware; rather choosing to force the application to be defined and allocated as either hardware or software; making the DO-254 method less ambiguous and more robust. That allocation provides the means to apply appropriate design considerations and leaves no room for interpretation. For those applications allocated to software, the governing design considerations are contained within DO-178B. In fact DO-178B and DO-254 are nearly equivalent in terms of development process considerations; however there are unique concerns in DO-254 that deal with the nature of hardware devices.

IEEE 7-4.3.2 contains multiple references to software and firmware, which is technically out of scope of DO-254; however, some of the software discussions can be related to the development of complex electronic hardware and, therefore, are discussed as best as can be determined throughout this report. Note that the nuclear power industry has an advantage in that massive physical redundancy is considered an appropriate and desired fault mitigation technique and such is inherent in the corresponding standards for 'system integrity'. However, DO-254, being an airborne avionics standard may not have those luxuries due to weight and size (physical) constraints.

The remainder of this section discusses IEEE 7-4.3.2 as the primary item, and then comparisons are made to the guidance provided by DO-254.

### ***a. Safety Assessment Process***

IEEE 7-4.3.2 is not developed around FAA-type practices regarding the System Safety Assurance (SSA) process. Safety assurance is driven by IEEE Std 603-1998. The DO-254 design assurance process is based on the substantiation that appropriate measures have been followed to assure functions are designed with safety and determinism for the level of assurance required for the intended aircraft function; for this, safety assessment is to be an iterative process throughout the product life cycle, starting with system safety practices at the front end of the development life cycle in order to substantiate the design assurance level for the hardware and provide objective evidence for such. It is outside the scope of this report to determine if IEEE Std 603-1998 provides an iterative safety assessment process.

The safety guidelines and methods listed in SAE ARP 4761 are the traditional precursor to DO-254 complex electronic hardware development and include Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Common Cause Analysis (CCA) among the techniques for system safety. DO-254 does not specify the details of these plans.

IEEE 7-4.3.2 provides a discussion centered on the identification and resolution of hazards as part of Annex D. Annex D provides detail into the hazard analysis process and also presents a brief discussion on the use of FTA and FMEA and they appear to be closely aligned with those considerations of SAE ARP 4761. A separate detailed analysis would be necessary to confirm similarities and differences between SAE ARP 4761 and IEEE 7-4.3.2 Annex D.

IEEE 7-4.3.2 provides a discussion centered on computer reliability and quantifiable reliability goals as part of Annex F. Included is a very general discussion describing that an evaluation of the development process can minimize the



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

existence of computer failures. The details of these aspects, including the use of anomaly reporting are at the essence of the design assurance guidance of DO-254, but not specifically related to reliability as is discussed in IEEE 7-4.3.2. DO-254 discusses reliability as associated with safety requirements addressed from a system perspective, to determine the required level of reliability and the level of assurance necessary to satisfy reliability requirements. The system perspective is iteratively assessed as hardware and software requirements are refined and derived throughout the development lifecycle. In addition to fault tree analysis, common mode analysis, and failure modes and effects analysis, statistical reliability analysis methods are referenced for applicable quantitative assessment of random faults, however the techniques for these statistical reliability analyses are not described in DO-254. It is implied that these analyses and assessments occur iteratively throughout the product development life cycle.

### ***b. Hardware Plans***

IEEE 7-4.3.2 does not directly identify enumerated hardware planning data to substantiate deterministic development that is consistent and repeatable for each facet of the design life-cycle process as detailed in DO-254. IEEE 7-4.3.2 does, however, reference plans such as a quality assurance plan and a configuration management plan. Additionally, IEEE 7-4.3.2 identifies a risk management plan, where DO-254 discusses the mitigation of risk as an iterative process through the development lifecycle based on the design assurance level. Product life cycle development standards are not described in IEEE 7-4.3.2. While IEEE 7-4.3.2 is considered a standard, it is an industry standard and not developed specifically to the unique development project. DO-254 requires the description and documentation of standards to be uniquely applied to the specific project

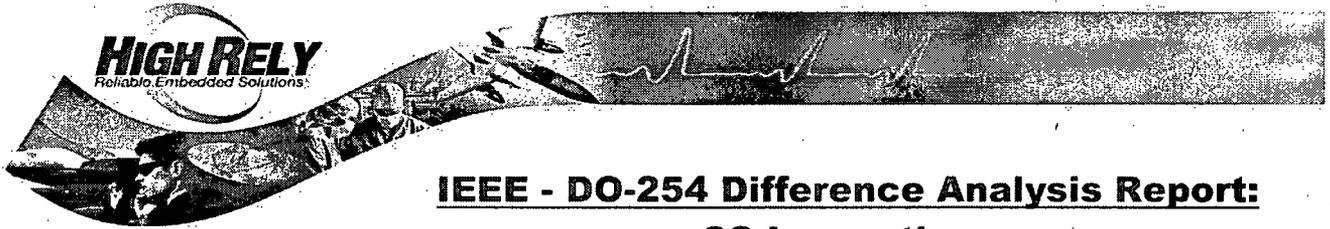
The complete set of DO-254 Hardware Planning data includes the Plan for Hardware Aspects of Certification (PHAC), the Hardware Design Plan (HDP), the Hardware Process Assurance Plan (HPAP), the Hardware Configuration Management Plan (HCMP), and the Hardware Verification and Validation Plan (HVVP), along with the project specific standards, including Hardware Requirement Standards, Hardware Design Standards, Hardware Implementation Standards, Hardware Validation and Verification Standards, and Hardware Archive Standards.

Customers regularly use the basic HighRely hardware planning data templates as the basis for their hardware planning and DO-254 compliance; tailoring these templates to their unique projects.

Planning for the use of Commercial off the Shelf (COTS) items is discussed in IEEE 7-4.3.2. DO-254 discusses the planned use of COTS in the PHAC, as "additional considerations". These additional considerations assure that COTS components will be verified through the overall design process, including the supporting processes. The use of an electronic component management process, in conjunction with the design process, provides the basis for COTS components usage. Often, the supporting processes are glanced over by the non-experienced reader. The supporting processes effort is not trivial. COTS components must meet the intent of DO-254.

DO-254 also provides great detail describing the technique of analyzing functional failure paths (FFP) and fail-safe aspects as part of the highest design assurance levels. Functional failure path analysis is often considered the 'cousin' to software structural coverage for complex electronic hardware. When used, FFP analysis provides the means to analyze every functional path throughout a hardware component and the combination of hardware components within the defined system. Each path possible in delivering any particular result based on any input combinations is individually analyzed to assure correct functional operation.

The relationship between the aviation certification authority, the Federal Aviation Administration (FAA) or designee, is not the same for nuclear power generating stations. In this capacity, the system developer liaises with the specific nuclear power generating station, who then liaises with the Nuclear Regulatory Commission (NRC). To draw a parallel, the planning provided by the PHAC could be used as an adequate medium between the developer and the nuclear power generating station. The nuclear power generating station in turn could use the 'PHAC-equivalent' plan



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

as a medium, similar to the FAA 'cert liaison' process, for explanation and discussion with the NRC regarding the plans for development of complex electronic hardware components destined to implement the requirements specified in the system design and specification data. Ultimately the results presented in Hardware Accomplishment Summary (HAS) provided at the completion of the development project could similarly communicate the accomplishments of the overall project and any variations from those plans presented in the PHAC.

### ***c. Hardware Conceptual Data***

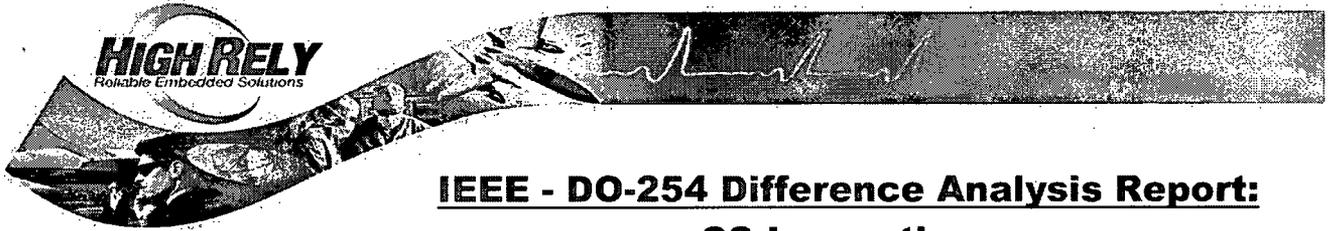
IEEE 7-4.3.2 does not detail the process of the conceptual data developed for complex electronic hardware, rather refers to the creation of the conceptual design of the system in the discussion of quality. It is presumed that either IEEE standards similar to IEEE 12207.0-1996 or IEEE 603-1998 provide detail with respect to hardware, but an in-depth difference analysis is outside the scope of this study. IEEE 7-4.3.2 describes software quality metrics to be considered throughout the software development life cycle, including correctness/completeness during the requirements phase, but does not discuss the means by which correctness and completeness is measured or determined. This is an example where the allocation of requirements to either hardware or software (i.e. not firmware) provides significant value. The development of decision making aspects (logic) of complex electronic hardware (PLDs, FPGAs, ASICs, etc...), while similar to software, is intended to be controlled under the auspices of DO-254; not DO-178B. Indeed, the guidance provided by both DO-254 and DO-178B are very similar; however there are aspects that are unique to DO-254 for the development of complex electronic hardware. It appears that the IEEE standards do not make that distinction; at least not within IEEE 7-4.3.2.

The concepts behind the product and its complex electronic hardware are elucidated and documented under the guidance of DO-254. The hardware conceptual data described in DO-254 includes architectural constraints related to safety, including those necessary to address design errors and functional, component over-stress, reliability and robustness defects and identifies implementation constraints on system components. Major components are identified. The way the major components contribute to the hardware safety requirements are determined, including the impact of unused functions. Derived and refined requirements, including the interface definition, are related and iteratively included in the system and hardware/software requirements. Requirement omissions and errors are fed back within the development life cycle for appropriate resolution based on their source. The development life cycle is prescribed so as to ensure that these errors and omissions are found. The reliability, maintenance, and test features to be provided are identified.

DO-254 guidance for high design assurance levels includes conceptual data and associated standards for representation of design data, and suggests that these are incorporated into development practices. HighRelY finds this practice also to be a very cost-effective process improvement on all programs; even those without high design assurance level requirements.

### ***d. Hardware Detailed Design Data***

IEEE 7-4.3.2 does not describe the detailed design data that describes the functions of the code blocks within the FPGA designs, however it does discuss software development under the guidance of IEEE 12207.0-1996. IEEE 7-4.3.2 discusses the use of the requirements to develop a detailed system design as part of the quality discussion. Further, IEEE 7-4.3.2 describes software quality metrics to be considered throughout the software development life cycle, including compliance with requirements at the design phase and it is presumed that these are applicable to FPGA designs. Since Annex D of IEEE 7-4.3.2 discusses the identification and evaluation of hazards during the detailed design phase, it is presumed that the detailed design phase is adequately specified in other IEEE standards. DO-254 is less concerned with such metrics than the IEEE standard, leaving the metric collection definition and collection process to the Production (Quality) Assurance organization.



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

The ability to modify the implementation can be severely hampered by the lack of detailed design data providing the why, what and the how of the design. DO-254 provides great detail into the detailed design aspects, including the detailed design objectives and the detailed design process activities, as well as the objective evidence to be developed, configured, and assured according to project plans and standards.

### ***e. Hardware Implementation (specific to FPGA)***

IEEE 7-4.3.2 does not directly address complex electronic hardware implementation. The standard is oriented toward system level considerations, with general discussions about software implementation as a function of system quality. As such, the software quality metrics references life cycle phase characteristics and demands that the implementation be compliant with the design. In this respect DO-254 and IEEE 7-4.3.2 are very similar.

DO-254 provides that a hardware item should be produced using the design data and, where practical, also using the resources intended for the production product, including procurement, kitting, build, inspection and test. Derived requirements generated by the implementation process are part of the overall, iterative life cycle process provided by DO-254. These requirements may have impact to the detailed design process, the requirements process or other appropriate processes. As well, errors and omissions discovered during the implementation process are identified, analyzed and provided to the appropriate process for resolution and continuation of the development process.

In addition, DO-254 discusses the production transition process needed to provide consistent, regular replication of the hardware item. As digital systems intended for use in nuclear power generating systems are not anticipated to be developed in a production line style, production transition may not completely apply; nonetheless, developers would do well to consider these aspects as part of installation and operation of these systems.

### ***f. Validation and Verification Process***

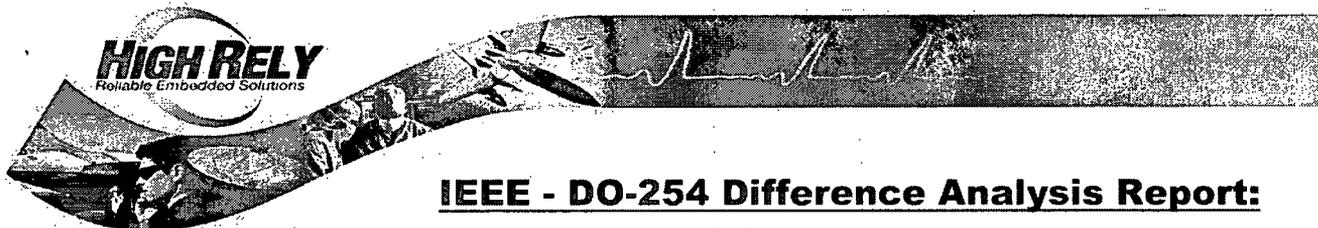
IEEE 7-4.3.2 does not provide great detail into the verification and validation processes for complex electronic hardware, but does reference IEEE Std 1012-1998, the IEEE Standard for Software Verification and Validation. In addition, IEEE 7-4.3.2 discusses verification and validation as a function of quality and as an extension of the program management and system engineering team activities used to identify objective data and draw conclusions about quality, performance and development process compliance. While no verification or validation planning is directly mentioned in IEEE 7-4.3.2, the mention of development process compliance from a quality perspective implies the development of plans for verification and validation and adherence to those plans.

Validation, from the perspective of DO-254, provides assurances that the hardware item derived requirements are correct and complete with respect to system requirements allocated to the hardware item. Verification, from the DO-254 perspective, provides assurance that the hardware item implementation meets all of the hardware requirements, including derived requirements. At the system level, then we can extrapolate that verification ensures that the system is correctly and completely developed to the specified requirements. Validation at the system level ensures that the requirements specified were, indeed the correct requirements for the system.

DO-254 specifically lays out the objectives, process and activities for both verification and validation, and these objectives, processes and activities support the definitions above.

IEEE 7-4.3.2 references IEEE Std 1012-1198 and mentions the 'highest integrity level (level4)'. It is presumed that the level 4 integrity equates to Level A criticality discussed within the aviation community and specifically within DO-254.

The organizational independence criteria identified in IEEE 7-4.3.2, specifically that "development and tests shall be verified and validated by individuals or groups... other than those who developed the original design", is directly



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

proportional to the guidance provided by DO-254 for level A critical systems. IEEE 7-4.3.2 specifically calls out the need for independently selecting the verification and validation techniques.

DO-254 also provides for advanced verification methods, including elemental analysis, safety-specific analysis, and formal methods. DO-254 suggests these analyses are applied and occur iteratively throughout the development life cycle and details are provided for each analysis or method. The Functional Failure Path Analysis is used to support these advanced verification methods and analyses and is well suited to ensure correct operation, without introduction of error or unintended function. Data from the analysis is used as a means of design assurance applicable to the hardware circuits, components, and elements, their internal functions, and their interconnectivity in the completed system.

### ***g. Configuration Management Practices***

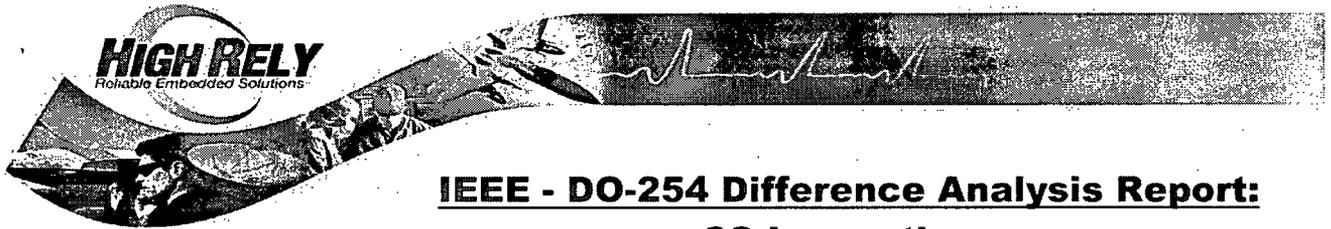
IEEE 7-4.3.2 identifies good practices for CM as part of the quality discussion. The discussion is targeted specifically at software configuration management. For the purposes of this report, we will extrapolate that to include the development of complex electronic hardware. It is presumed that the IEEE Std 1042-1987 and IEEE Std 828 provides guidance for well defined release structure, naming conventions, baseline control, release practices, and use of rudimentary tools to provide baselines of release. What is not evident is whether these practices are applied for "in-process" CM control baselines and whether they apply to development data. This is implied by the statement that software baselines are established at "appropriate points" in the software life cycle process, but "appropriate points" is a nebulous term. We can presume that the appropriate points would be more clearly refined in the software configuration management plan developed under the guidance of IEEE Std 1042- 1987 (R1993) and 828 - 1998, but cannot ensure that the rigor of the design guidance of DO-254, including configuration management methods, baselines, problem reporting and resolution, change control, storage and retrieval, environmental control and configuration management tools are included in such a plan; or that they would be applied to development data.

IEEE 7-4.3.2 also refers to baseline control in that 'approved changes' that are created shall be added to the baseline, but does not specify the approval authority for those changes. It is presumed that the software configuration management plan developed under guidance of IEEE Std 828 - 1998 will establish the change control authority and the multiple release strategy.

The software configuration management discussion in IEEE 7-4.3.2 describes a minimum set of activities, starting with identification and control of all software designs and code. What is not evident is the identification and control of requirements on which the designs and implementation are based; that is, the system, software, and hardware requirements. Apparent is the control of user, operating and maintenance documentation and that fulfills the some needs described in DO-254 for production transition to in-use operation. Also apparent in IEEE 7-4.3.2 is the control of vendor development activities for supplied safety system software. It is presumed that this includes ensuring equivalent processes from vendors, as is indicated in DO-254 discussions regarding compliance substantiation of both supplier development and COTS.

IEEE 7-4.3.2 describes equipment qualification and this is not unfamiliar to developers who use the guidance of DO-254. In fact, qualification is achieved using the vehicles of the Hardware Configuration Index (HCI) to identify those components (and their internal configuration) which are intended for use in actual operation, as well as the Hardware Environment Configuration Index (HECI) to identify those components and tools used in the development and testing of the HCI. The intent is to be able to repeat results consistently by insuring the overall configuration is identified and does not change.

Configuration audits and configuration status accounting are identified as important objectives in both IEEE 7-4.3.2 and DO-254; however the auditing function is discussed in DO-254 as a function of the process assurance practices.



## **IEEE - DO-254 Difference Analysis Report:** **CS Innovations**

### ***h. Process Assurance Practices***

IEEE 7-4.3.2 does not directly address process assurance, but does identify quality assurance as a principal theme. For all intents and purposes, DO-254 process assurance objectives are quality assurance exercises. IEEE 7-4.3.2 recognizes the need for a quality assurance plan, but refers to IEEE Std 730 – 1998 and IEC 60880 (1986-09) [B4] for the details of that plan. IEEE 7-4.3.2 suggests an approved quality assurance plan compatible with the requirements of IEEE/EIA 12207.0-1996. Approval authority is not specified.

IEEE 7-4.3.2 provides assurance that the required computer system hardware and software are installed in the appropriate system configuration; that firmware and software identification is used to assure correct installation in the correct hardware component, that the software identification can be retrieved from the firmware, and that physical identification requirements meet the identification requirements of IEEE Std 603-1998. There is little doubt that these criteria are, if not completely, nearly compliant with the guidance of DO-254, but further analysis outside the scope of this report would be required to confirm this.

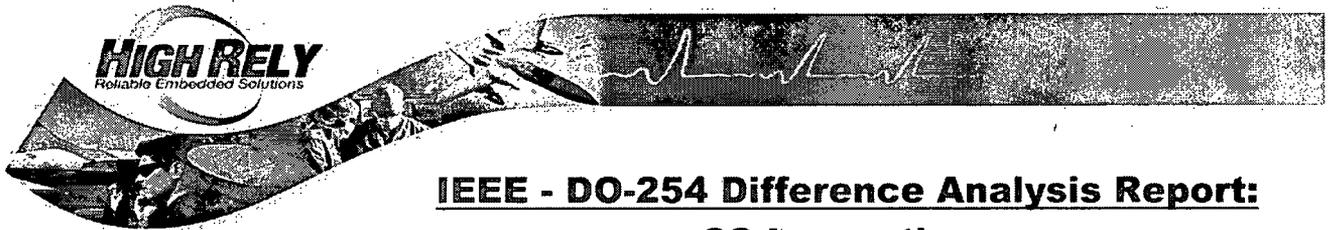
In addition, IEEE 7-4.3.2 presents a need for quality assurance surrounding the diversity requirements of safety systems and the need for diversity to mitigate the risk of common mode failures; although this is more of a safety system specification exercise than a development process exercise. The independent nature of quality (process) assurance is addressed in both IEEE 7-4.3.2 and DO-254 design assurance for the highest (Level A) criticality.

Transition criteria, methods and strategies for assurance that life-cycle processes are not directly addressed as part of the IEEE 7-4.3.2 criteria. The process assurance process presented in DO-254 presents processes checks, transition criteria, when and where they are conducted relative to the complex electronic hardware design, implementation, and testing stages; and identifies process assurance records to be retained as objective evidence of compliance. The same applies to audits: all of the DO-254 related processes and artifacts described are to be audited; the audit points, frequency, depth, and record keeping (checklists) are identified as part of the Hardware Process Assurance Plan (HPAP).

The quality of the hazard analysis is addressed within IEEE 7-4.3.2 and the assurance that the design is enveloped within the identified system constraints is presented along with assurances that non-safety software modules do not adversely affect safety system modules. This is commonly referred to as partitioning of criticality level within aviation systems which are subject to the guidance of DO-254 and DO-178B and can be achieved through architectural mitigation. Architectural mitigation also includes dissimilar implementation, redundancy, monitors, isolation, and command/authority limits specifically employed to mitigate or contain the adverse effects of hardware design and implementation errors. These techniques are employed throughout the development life cycle, but are most cost effective when presented during system design and allocation. Note that DO-254's Production Assurance is basically a Quality Assurance process, applied through development and manufacturing.

### ***i. Certification Liaison***

IEEE 7-4.3.2 does not identify a Cert Liaison activity. The relationship of the Nuclear Regulatory Commission (NRC) to the individual nuclear power generating stations and the suppliers of system equipment integrated into those stations is tightly coupled due to the severe nature of potential system failures and the limited number of nuclear power generating stations operating throughout the country. In contrast, there are many aviation systems deployed on a great number of airborne platforms. The individual nuclear power generating station is closely engaged and, in effect performs the cert liaison function that a Designated Engineering Representative (DER) and/or



## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

Designated Airworthiness Representative (DAR) perform for aviation systems development under the auspices of the Federal Aviation Administration (FAA).

Under the guidance of DO-254, the Cert Liaison activity is identified to assure that the development project is well planned; objective evidence starts with the PHAC as the proposed means of compliance. The cert liaison activity assures that the development project is developed and controlled according to plan, and that the compliance is substantiated; objective evidence of substantiation is presented in the Hardware Accomplishment Summary (HAS). In effect, the PHAC and the HAS become 'book-ends' that surround the development project and force rigid communication to the cert authority of compliance with regulatory and project objectives. These methods have served the aviation industry well.

The tightly coupled and controlled communication between the NRC, individual power generating stations and the developer of station sub-system has served the nuclear power industry equally as well, it seems, but the addition of these plans could serve to increase awareness and communication for development projects associated with complex digital systems throughout the development life cycle.

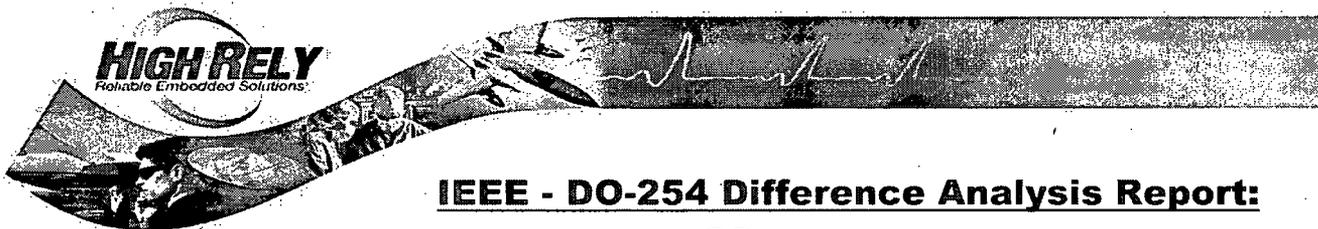
### **2.2 Summary of IEEE 7-4.3.2 and DO-254**

The principal difference between IEEE 7-4.3.2 and DO-254 relates to the scope of each document. IEEE 7-4.3.2 serves to amplify criteria established in multiple other IEEE standards as a means of addressing safety systems in nuclear power generating stations; the emphasis being on the system level. The criteria of IEEE 7-4.3.2 principally addresses functional and design requirements for computers used as components of these safety systems and does not specifically address the in-process design considerations of such systems; rather leaving those details to the other IEEE standards.

DO-254 addresses the specific design considerations and provides design guidance for each phase of the development life cycle; the emphasis being on the development processes once the system requirements are specified to ensure that the complex electronic hardware performs its intended function correctly and does not introduce errors or unintended function, while providing a vehicle to identify incorrect or incomplete system specification along with other ambiguities that may only be discovered once the development process has proceeded. In other words, DO-254 prescribes feedback within the scope of the development life cycle to the system aspects used as a basis for that development. An in-depth difference analysis could identify clearly the in-process, development life cycle differences between DO-254 and the other IEEE standards mentioned in IEEE 7-4.3.2.

### **2.3 Conclusion**

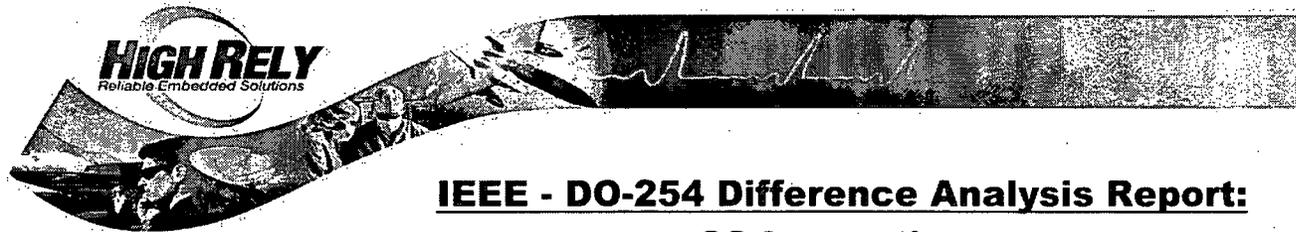
It is apparent that IEEE 7-4.3.2 provides excellent engineering guidance and when coupled with the other referenced documents provides for the definition and development of safety systems while mitigating risk of failure throughout the development life cycle. There is little question that the guidance of these standards is sound. DO-254 also provides quite similar guidance, but does not provide the detail in the area of risk management and risk mitigation in a concise section, as does IEEE 7-4.3.2. Risk mitigation and management under DO-254 is integral to the entire development life cycle and is apparent given the iterative nature of the development processes. The secret for all projects is in achieving compliance efficiently and cost-effectively. This analysis has highlighted the differences between IEEE 7-4.3.2 and DO-254 and pointed also to their similarities. Details for each section of DO-254 are provided in the tables which follow.



**IEEE - DO-254 Difference Analysis Report:**  
**CS Innovations**



***HighRelY Avionics & Certification Center***  
***Phoenix, Arizona***



## **IEEE - DO-254 Difference Analysis Report:**

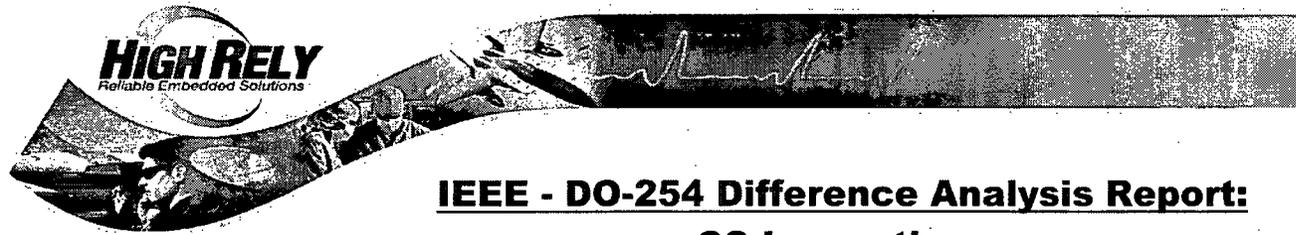
### **CS Innovations**

## **3 Complex Electronic Hardware (CEH) Difference Analysis**

### **3.1 Hardware (ASIC/PLD) Planning Process**

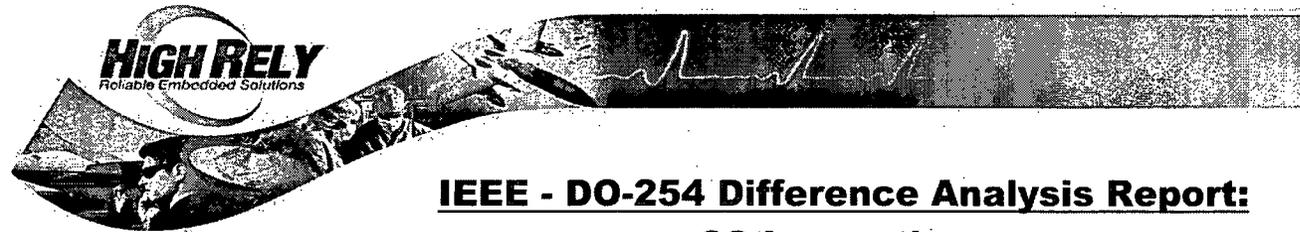
(Section 3)

<b>DO254 Reference</b>	<b>Objective Description</b>	<b>Output Data</b>	<b>Applicable Level</b>	<b>Difference Analysis Findings</b>	<b>Comments</b>
4.1 (1)	The hardware design life cycle processes are defined.	PHAC (10.1.1) HDP (10.1.2) HVP (10.1.3)	All	IEEE 7-4.3.2 does not define life cycle processes in detail, but discusses them generally as part of quality discussions.	Life cycle processes are referenced, but the definition is contained in other IEEE Standards
4.1 (2)	Standards are selected and defined.	HVVP (10.1.4) HCMP (10.1.5) HPAP (10.1.6) HW Req.Std. (10.2.1) HW Des.Std. (10.2.2) HWV&V Std. (10.2.3)	All	IEEE 7-4.3.2 does not identify standards.	Program-level standards are not identified; whether the standards referenced would satisfy program-level objectives is out of scope of this study.
4.1 (3)	The hardware development and verification environments are selected or defined.	HW Arch.Std. (10.2.4)	All	IEEE 7-4.3.2 does not define development environments but discusses a project environment suitable for effective communications between individuals and groups for the resolution of software project risks as part of the quality discussions. Development environments are also discussed as a potential source of origination of hazards.	



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
4.1 (4)	The means of compliance of the hardware design assurance objectives, including strategies identified using guidance in Section 2.3.4, are proposed to the certification authority.		All	IEEE 7-4.3.2 does not propose means of compliance such as PHAC and HAS.	This practice helps ensure end-to-end success and communication with certification authorities.

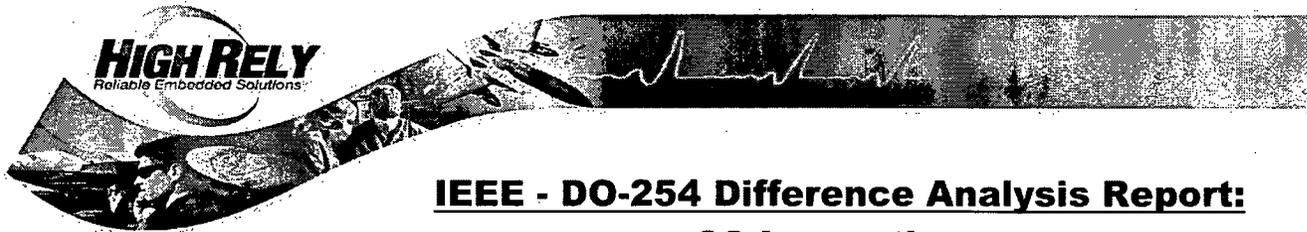


## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

### **3.2 Hardware (ASCI/PLD) Architectural Decisions**

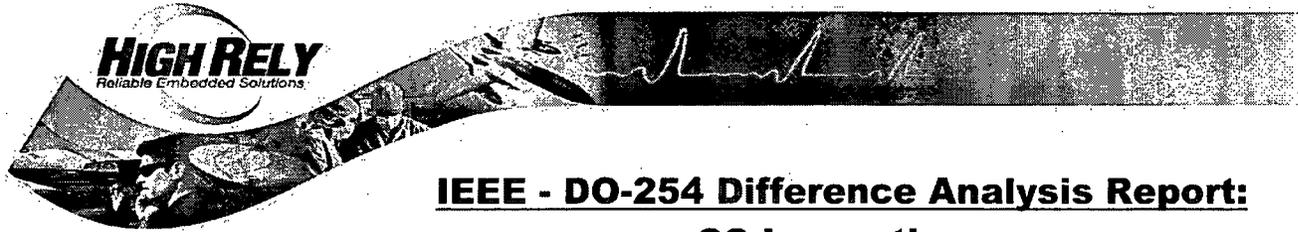
(Section 2.3)

<b>DO254 Reference</b>	<b>Objective Description</b>	<b>Output Data</b>	<b>Applicable Level</b>	<b>Difference Analysis Findings</b>	<b>Comments</b>
2.3.1(1)	Iterative hardware safety assessment and design should determine derived hardware safety requirements and ensure that system safety requirements allocated to the hardware are satisfied and ensure that derived requirements are satisfied.	Requirements Standards  Trace Data  High-Level Design  HPA standards.	All	IEEE 7-4.3.2 has safety systems as its principal focus, but does not address the iterative nature of the safety assessments throughout the development life cycle.	



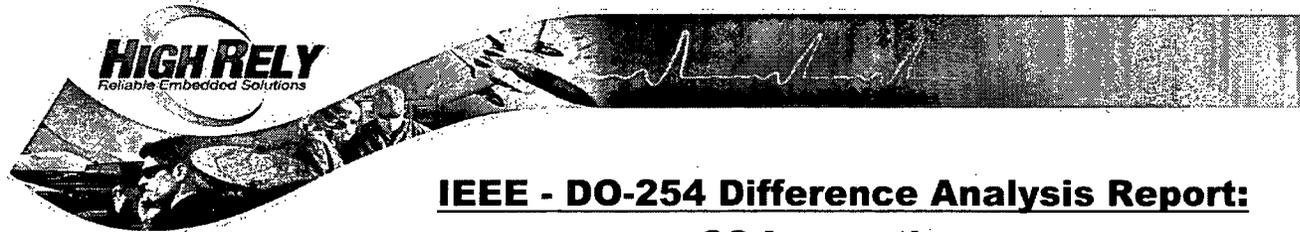
**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
2.3.1(2)	These derived requirements should include safety requirements for hardware architecture, circuits and components, and protection against anomalous behaviors, including incorporating specific hardware architectural and functional safety attributes,		All	IEEE 7-4.3.2 has safety systems as its principal focus, but does not specifically address derived requirements throughout the development life cycle.	Derived requirements ensuring that safety, reliability and functional aspects should be mitigated through architectural means and established as defined, traceable items throughout the development life cycle.



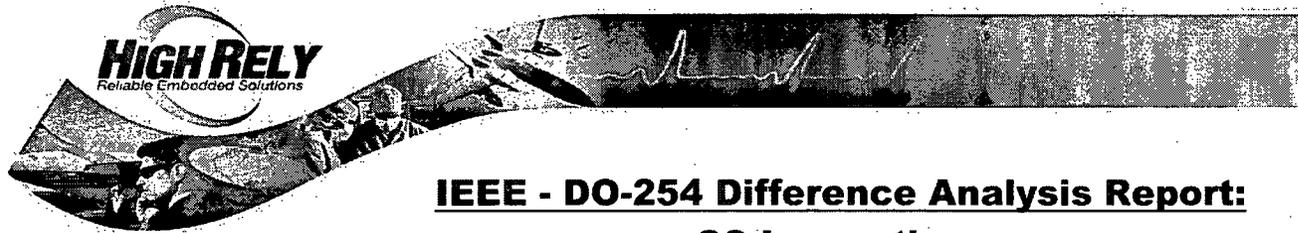
**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
2.3.1(3)	The hardware design assurance process and the hardware safety assessment should jointly determine the specific means of compliance and design assurance level for each function and should determine that an acceptable level of design assurance has been achieved.			IEEE 7-4.3.2 does not discuss design assurance levels.	Digital Computers in Safety Systems of Nuclear Power Generating Stations are of the highest criticality.
2.3.2	Quantitative Assessment of Random Hardware Faults			IEEE 7-4.3.2 Annex D discusses random faults as an aspect of identification and resolution of hazards.	"Either quantitative or qualitative judgment of the probability of occurrence should be sufficient to determine if further action is required"



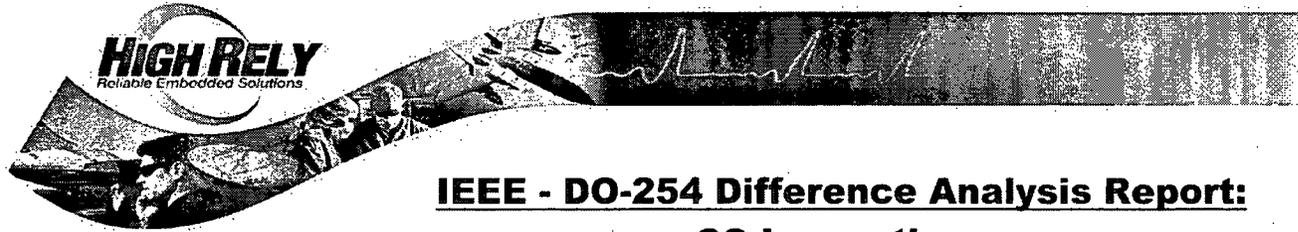
## IEEE - DO-254 Difference Analysis Report: CS Innovations

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
2.3.3	Qualitative Assessment of Hardware Design Errors and Upsets	Safety Assessment Hardware Design Data	All	IEEE 7-4.3.2 Annex D discusses hardware design errors as an aspect of identification and resolution of hazards.	Example: "undesired consequence may in turn be used as the top event in a FTA, which would then be decomposed to lower-level intermediate events and terminated in the lowest level of design for which qualitative or quantitative probabilities could be assessed"
2.3.4(1)	For Level A or B functions implemented in hardware, the design assurance considerations should address potential anomalous behaviors and potential design errors of the hardware functions.	Safety Assessment, Hardware Design Data	A/B	IEEE 7-4.3.2 Annex D discusses hardware design errors as an aspect of identification and resolution of hazards. Annex F discusses computer reliability and directly discusses unanticipated behavior, failure/error handling, or timing and processor loading	"Anomalous behaviors" is not directly mentioned.



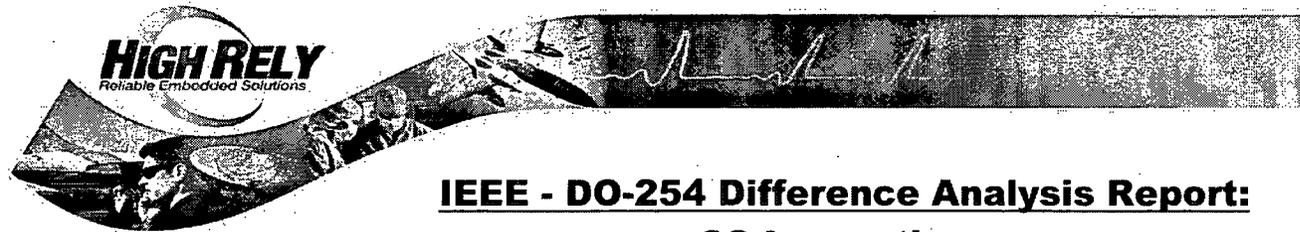
**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
2.3.4(2)	The decision making process outlined in Figure 2-3 should be used when developing design assurance strategies for each hardware function being implemented.	Design Assurance Data	All	IEEE 7-4.3.2 is related to systems of the highest criticality and as such does not provide a decision making process for determining varying levels of design assurance strategies. IEEE 7-4.3.2 does refer to interaction with non-safety systems as part of Annex D discussion on the potential introduction of hazards	The equivalent decision is level A and design assurance strategies would fall under that category, at a minimum.
2.3.4(3)	The strategies described in Appendix B should be applied for Level A and B functions in addition to the guidance provided in Section 3 through Section 11.	Safety Assessment, HW Design Data, Architectural Design Data	A/B	IEEE 7-4.3.2 does not directly address functional failure path analysis, architectural mitigation, product service experience, or advanced verification methods such as elemental analysis, safety-specific analysis, and formal methods related to functional failure paths.	



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

<b>DO254 Reference</b>	<b>Objective Description</b>	<b>Output Data</b>	<b>Applicable Level</b>	<b>Difference Analysis Findings</b>	<b>Comments</b>
2.3.4(4)	The design assurance strategy should be selected as a function of the hardware architecture and usage, and of the hardware implementation technology that has been chosen.	Standards, HW design data, Plans	All	IEEE 7-4.3.2 discusses hardware architecture in the section on safety system criteria and in Annex F section on computer reliability	

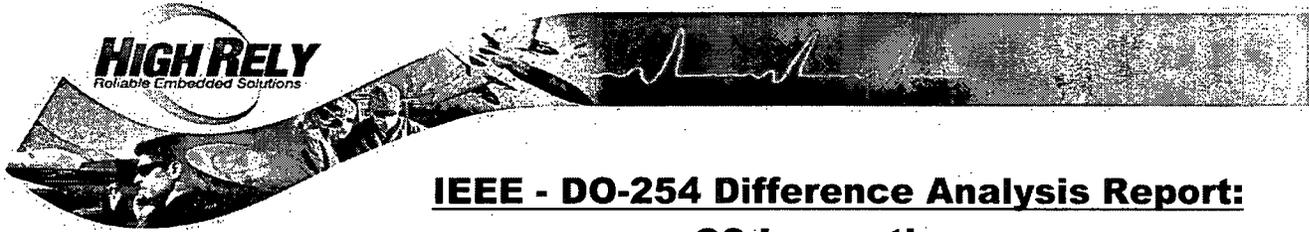


## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

### **3.3 Hardware (ASIC/PLD) Requirements Capture**

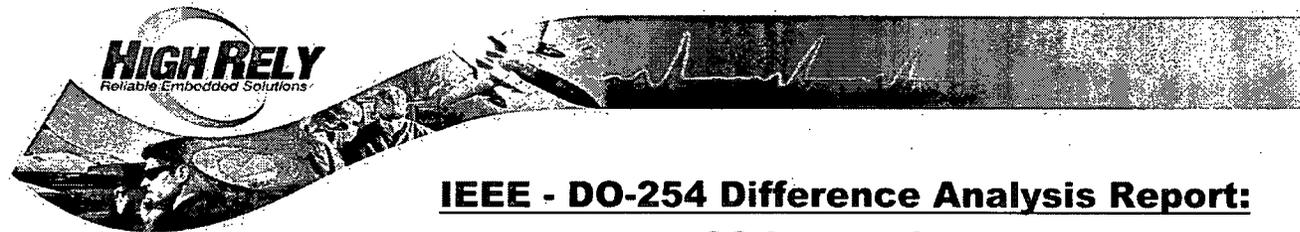
(Section 5.1)

<b>DO254 Reference</b>	<b>Objective Description</b>	<b>Output Data</b>	<b>Applicable Level</b>	<b>Difference Analysis Findings</b>	<b>Comments</b>
5.1.1(1)	Requirements are identified, defined and documented. This includes allocated requirements from the PSSA and derived requirements from the hardware safety assessment.	Hardware Requirements (10.3.1), Problem Reports (10.6)	All	IEEE 7.4.3.2 does not directly address the methods associated with the development of hardware requirements; nor the source of them. Software requirements steps are identified in section 5.4.2 , Qualification of existing commercial computers. Annex D discusses the relationship of software requirements to hazards.	In this case, we presume that software requirements are equivalent to complex electronic hardware requirements, so in essence the activity is performed.
5.1.1(2)	Derived requirements produced are fed back to the appropriate process.		All	Derived requirements are not mentioned in IEEE 7-4.3.2.	



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
5.1.1(3)	Requirement omissions and errors are provided to the appropriate process for resolution.		All	Errors and omissions are discussed as part of IEEE 7-4.3.2 Annex D (Identification and resolution of Hazards). It does not detail the process, but discusses it as a function of V&V under the general quality discussions and as an extension of program management and system engineering team activities.	Process discussions are contained within other IEEE standards.

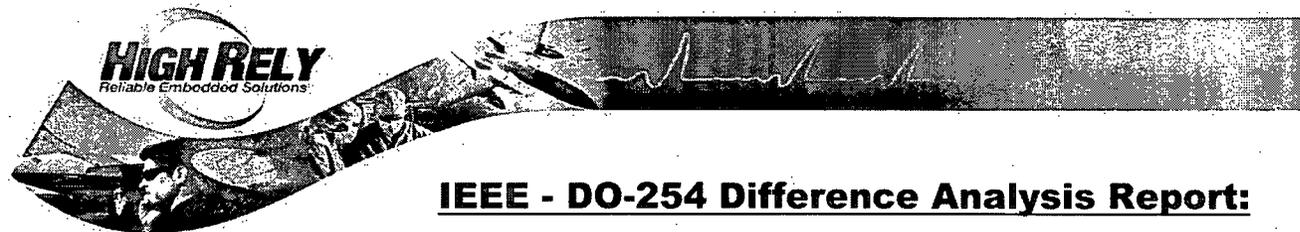


**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

**3.4 Hardware (ASIC/PLD) Preliminary Design (behavioral, Conceptual design)**

(Section 5.2)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
5.2.1(1)	The hardware item conceptual design is developed consistent with its requirements.	Conceptual Design Data (10.3.2.1), Hardware Requirements (10.3.1), Problem Reports (10.6)	All	IEEE 7-4.3.2 refers to the creation of the conceptual design of the system in the discussion of quality and the quality assurance plan. It does not detail the process of the conceptual data.	The quality discussion in IEEE 7-4.3.2 provides high-level discussions regarding life cycle processes, but does not discuss consistency, process feedback, tracing, etc...
5.2.1(2)	Derived requirements produced are fed back to the requirements capture or other appropriate processes.			IEEE 7-4.3.2 does not discuss derived requirements, but does discuss software quality and the quality assurance plan. It does not detail the process of requirements feedback, but discusses it as a function of V&V.	Do other IEEE standards address derived requirements?
5.2.1(3)	Requirement omissions and errors are provided to the appropriate processes for resolution.			IEEE 7-4.3.2 refers to problem resolution in the discussion of quality and the quality assurance plan. It does not detail the process, but discusses it as a function of V&V.	

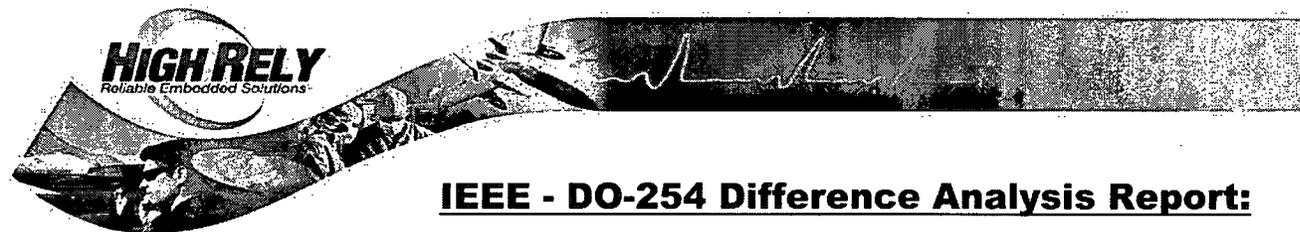


**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

**3.5 Hardware (ASIC/PLD) Detailed Design (synthesis, mask generation, fuse file)**

(Section 5.3)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
5.3.1(1)	The detailed design is developed from the hardware item requirements and conceptual design data.	Detailed Design Data (10.3.2.2) Top-Level Drawing (10.3.2.2.1) Assembly Drawing (10.3.2.2.2) Hardware/Software Interface Data (10.3.2.2.4)	All	IEEE 7-4.3.2 discusses detailed design as a function of quality and the quality assurance plan. IEEE 7-4.3.2 does not specifically define the links or trace process, but discusses process feedback as part of the V&V exercise.	It is presumed that these processes are included in other IEEE standards.
5.3.1(2)	Derived requirements are fed back to the conceptual design process or other appropriate processes.	Problem Reports (10.6)	All	IEEE 7-4.3.2 does not address derived requirements directly, but discusses the requirements, design and implementation processes as a function of quality and the quality assurance plan.	Do other IEEE standards address derived requirements?
5.3.1(3)	Requirement omissions or errors are provided to the appropriate processes for resolution.			IEEE 7-4.3.2 addresses errors and omissions as a function of introduced hazards. Process feedback is discussed as a function of V&V.	It is presumed that these process details are included in other IEEE standards.

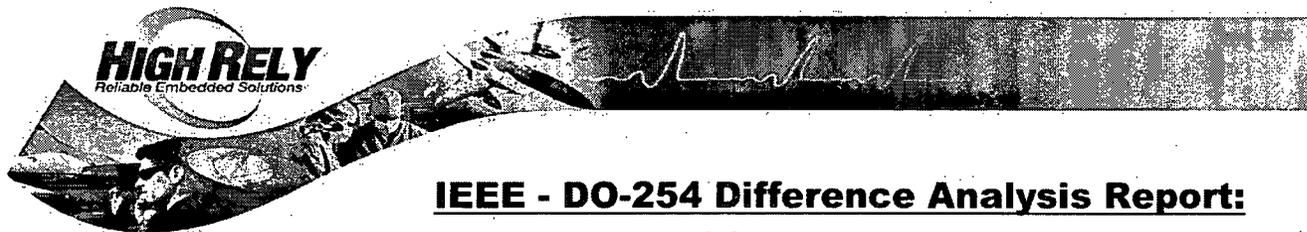


**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

**3.6 Hardware (ASIC/PLD) Fabrication (programming programmable components/Implementation)**

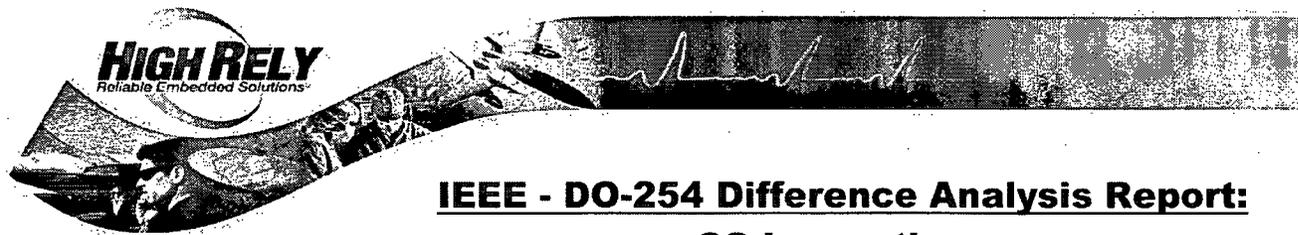
(Section 5.4)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
5.4.1(1)	A hardware item is produced which implements the hardware detailed design using representative manufacturing processes.	Installation Control Drawings (10.3.2.2.3), Problem Reports (10.6)	All	IEEE 7-4.3.2 does not directly address the representative manufacturing process.	Digital systems for nuclear power generation do not use mass-production manufacturing processes and are scrutinized closely on an individual bases.
5.4.1(2)	The hardware item implementation, assembly and installation data is complete.		All	IEEE 7-4.3.2 discusses implementation and assembly compliance with requirements (Installation and Checkout phase) as part of the quality discussion, within the discussion of commercial computers and within the discussion of functional hazards.	
5.4.1(3)	Derived requirements are fed back to the detailed design process or other appropriate processes.		All	IEEE 7-4.3.2 does not directly address derived requirements.	Do other IEEE standards address derived requirements?



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

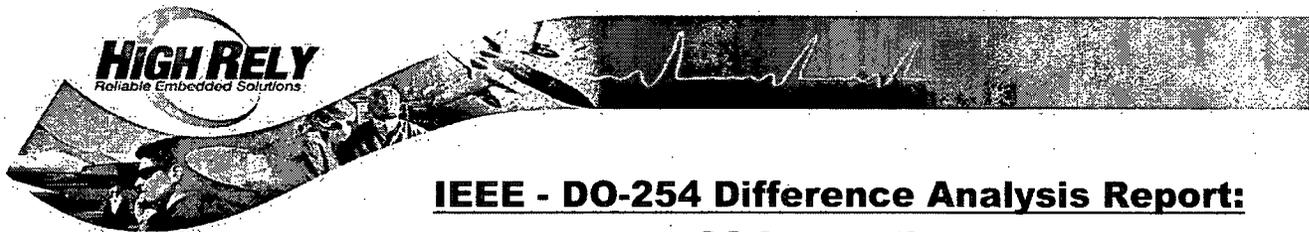
DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
5.4.1(4)	Requirement omissions and errors are provided to the appropriate processes for resolution.		All	IEEE 7-4.3.2 addresses errors and omissions as a function of introduced hazards. Process feedback is discussed as a function of V&V.	It is presumed that these process details are included in other IEEE standards.



## IEEE - DO-254 Difference Analysis Report: CS Innovations

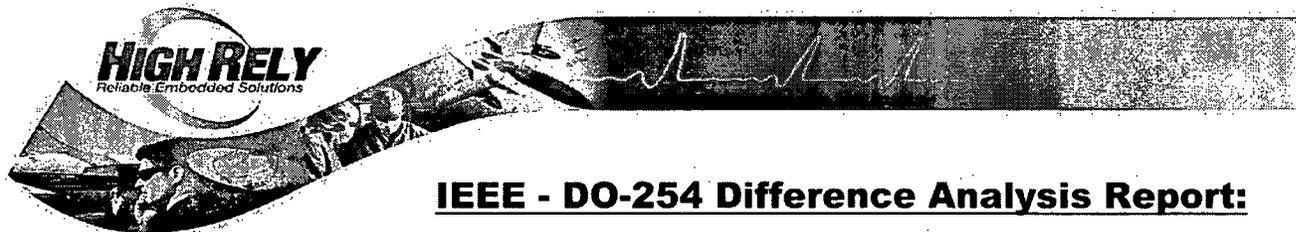
### 3.7 Hardware (ASIC/PLD) Production Transition (Section 5.5)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
5.5.1(1)	A baseline is established that includes all design and manufacturing data needed to support the consistent replication of the hardware item.	Hardware Requirements (10.3.1) Top-Level Drawing (10.3.2.2.1) Assembly Drawing (10.3.2.2.2) Installation Control Drawing (10.3.2.2.3) HW/SW Interface Data (10.3.2.2.4) Problem Reports (10.6)	All	IEEE 7-4.3.2 addresses baselines as part of its discussion about software configuration management plans in an effort to synchronize engineering and documentation activities at 'appropriate points'. It does not directly reference all design and manufacturing data or consistent replication.	Identification, control, audits and status accounting are all mentioned.
5.5.1(2)	Manufacturing requirements related to safety are identified and documented and manufacturing controls are established.	HW Configuration Management Records (10.7)	All	IEEE 7-4.3.2 does not directly address the representative manufacturing process.	Digital systems for nuclear power generation do not use mass-production manufacturing processes and are scrutinized closely on an individual bases.



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
5.5.1(3)	Derived requirements are fed back to the implementation process or other appropriate processes.		All	IEEE 7-4.3.2 addresses general process feedback as a part of the V&V discussion, but does not directly reference derived requirements.	
5.5.1(4)	Errors and omissions are provided to the appropriate processes for resolution.		All	IEEE 7-4.3.2 addresses errors and omissions as potentially introduced hazards. Process feedback is part of the V&V discussion.	

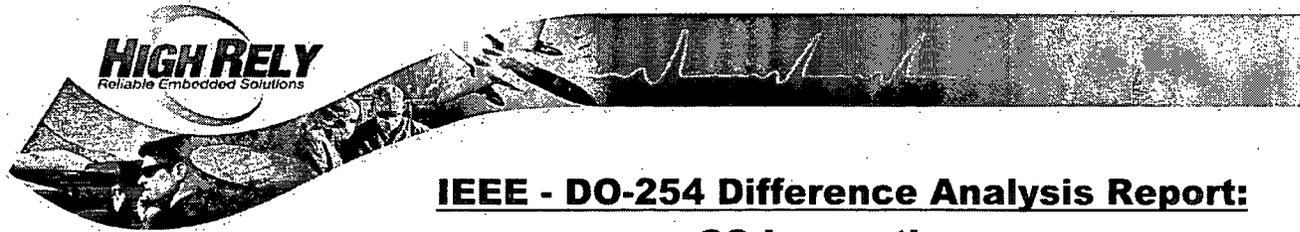


**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

**3.8 Hardware (ASIC/PLD) Validation and Verification (timing analysis, behavioral simulation, gate level simulation and design)**

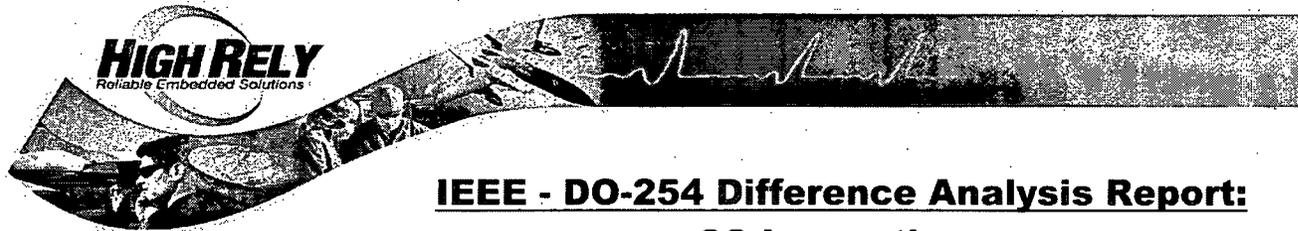
(Section 6)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
6.1.1(1)	Derived hardware requirements against which the hardware item is to be verified are correct and complete.	Hardware Trace Data (10.4.1) Hardware Review and Analysis Procedures (10.4.2) Hardware Review and Analysis Results (10.4.3) Hardware Test Procedures (10.4.4)	All	IEEE 7-4.3.2 does not directly address derived requirements or trace data development.	It is presumed that tracing through life cycle data is a part of other IEEE standards.
6.1.1(2)	Derived requirements are evaluated for impact on safety	Hardware Test Results (10.4.5) Hardware Acceptance Test Criteria (10.5)	All	IEEE 7-4.3.2 does not directly address derived requirements, but discuss impact of requirements and evaluation as part of the hazards discussions of Annex D	
6.1.1(3)	Omissions and errors are fed back to the appropriate processes for resolution.	Problem Reports (10.6)	All	IEEE 7-4.3.2 addresses feedback as part of V&V section under the general quality discussions and as an extension of program management and system engineering team activities.	Details are likely presented in other IEEE standards.



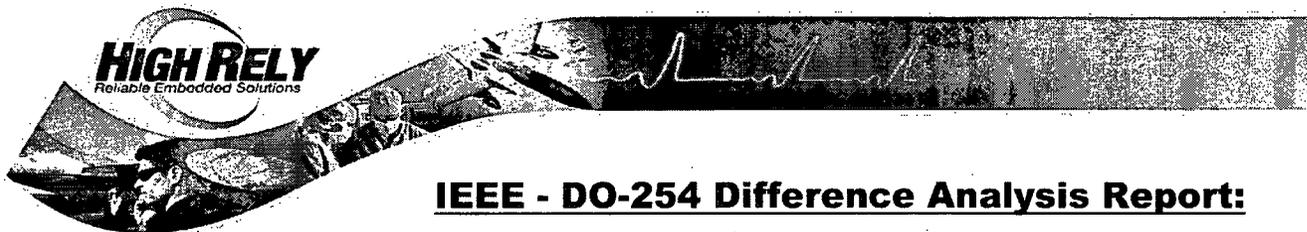
**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
6.2.1(1)	Evidence is provided that the hardware implementation meets the requirements.		All	IEEE 7-4.3.2 discusses acceptance based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions.	
6.2.1(2)	Traceability is established between hardware requirements, the implementation, and the verification procedures and results.		All	IEEE 7-4.3.2 does not directly address traceability except as related to COTS (section 5.4), but does infer that requirements, design and implementation must be verified.	It is presumed that other IEEE standards detail the traceability process



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
6.2.1(3)	Acceptance test criteria are identified, can be implemented and are consistent with the hardware design assurance levels of the hardware functions.	Hardware Acceptance Test Criteria (10.5)	All	IEEE 7-4.3.2 addresses acceptance testing as part of the quality discussions, but does not address consistency with design assurance levels.	Always the highest design assurance is presumed with digital systems for nuclear power generating stations.
6.2.1(4)	Omissions and errors are fed back to the appropriate processes for resolution.			IEEE 7-4.3.2 addresses errors and omissions and feedback as part of the V&V section under the general quality discussions and as an extension of program management and system engineering team activities.	

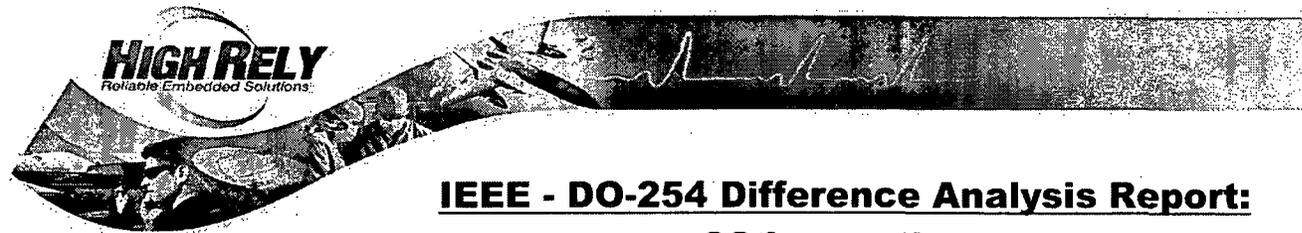


**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

**3.9 Hardware (ASIC/PLD) Configuration Management Process**

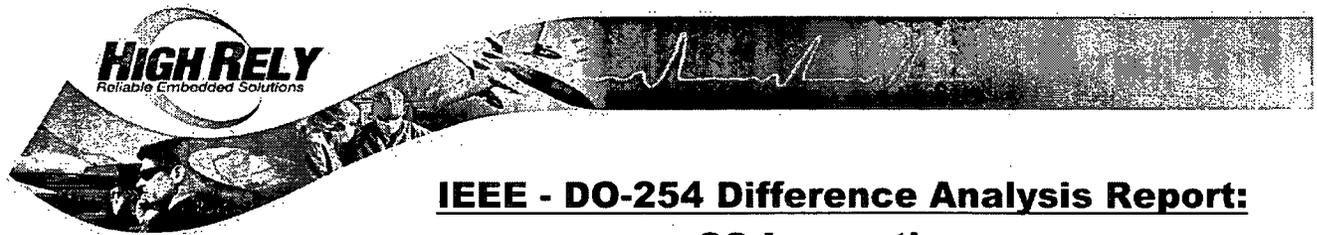
(Section 7)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
7.2(1)	Configuration items should be uniquely identified, documented and controlled. This may include, but is not limited to, hardware, design representations of hardware, tools or other data items used for certification credit and baselines	Problem Reports (10.6) Hardware Configuration Management Records (10.8)	All	IEEE 7-4.3.2 provides a section on configuration management under the auspices of quality, but also refers to IEEE Std 828 and IEEE Std 1042 as the primary sources.	
7.2(2)	Baselines should be established.		All	IEEE 7-4.3.2 addresses baselines	



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

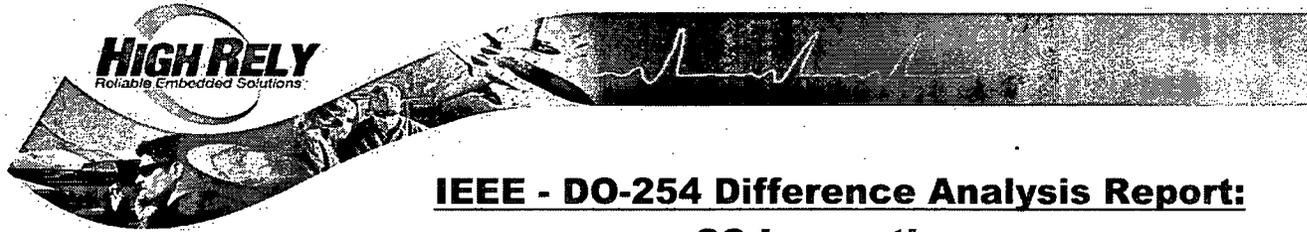
DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
7.2(3)	Problems should be uniquely identified, tracked and reported.		All	IEEE 7-4.3.2 addresses approval of changes to baselines.	This is inferred to include problem reporting and tracking.
7.2(4)	Change control and tracing of changes should be maintained. This requires that life cycle data identified in the plans should be secure and retrievable.		All	IEEE 7-4.3.2 addresses approval of changes to baselines.	This is inferred to include problem reporting and tracking.
7.2(5)	Archiving, retrieval and release of configuration items should be controlled.		All	IEEE 7-4.3.2 does not specifically addresses archiving.	It is presumed this data is discussed in IEEE Std 828 and IEEE Std 1042



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

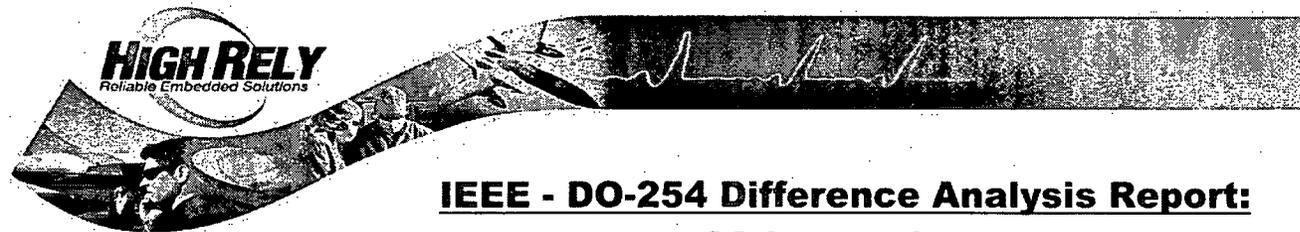
**3.10 Hardware (ASIC/PLD) Process Assurance**  
(Section 8)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
8.1(1)	Life cycle processes comply with the approved plans.	Hardware Process Assurance Records (10.8)	All	IEEE 7-4.3.2 does not provide guidance, other than program management as to the compliance to approved plans.	
8.1(2)	Hardware design life cycle data produced complies with the approved plans.		All	The closest that can be seen is IEEE 7-4.3.2 addresses through the discussion of software quality metrics: Correctness/Completeness (Requirements phase) Compliance with requirements (Design phase) Compliance with design (Implementation phase) Functional compliance with requirements (Test and Integration phase) On-site functional compliance with requirements (Installation and Checkout phase) Performance history (Operation and Maintenance phase)	



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
8.1(3)	The hardware item used for conformance assessment is built to comply with the associated life cycle data.		All	The closest that can be seen is IEEE 7-4.3.2 addresses through the discussion of software quality metrics: Correctness/Completeness (Requirements phase) Compliance with requirements (Design phase) Compliance with design (Implementation phase) Functional compliance with requirements (Test and Integration phase) On-site functional compliance with requirements (Installation and Checkout phase) Performance history (Operation and Maintenance phase)	

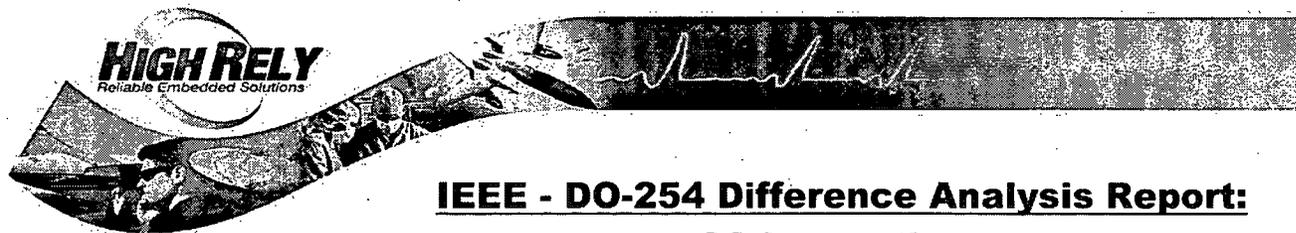


## **IEEE - DO-254 Difference Analysis Report: CS Innovations**

### **3.11 Hardware (ASIC/PLD) Certification Liaison Process**

(Section 9)

<b>DO254 Reference</b>	<b>Objective Description</b>	<b>Output Data</b>	<b>Applicable Level</b>	<b>Difference Analysis Findings</b>	<b>Comments</b>
9.1	The applicant proposes a means of compliance for hardware.	Hardware Accomplishment Summary (HAS) (10.9)	All	IEEE 7-4.3.2 does not include a means for compliance.	
9.2	The applicant provides evidence that the hardware design life cycle processes have satisfied the hardware plans.		All	IEEE 7-4.3.2 does not include discuss the evidence of satisfaction to approved plans outside the program management and V&V practices.	



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

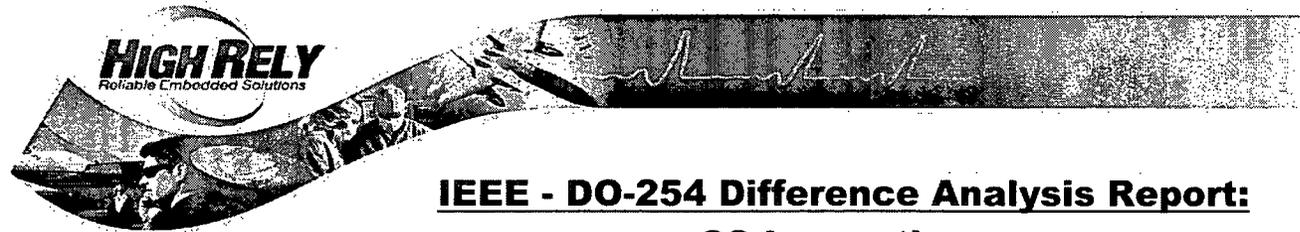
**3.12 Hardware (ASIC/PLD) Additional Consideration for Levels A&B**

(Appendix B)

DO254 Reference	Objective Description	Output Data	Applicable Level	Difference Analysis Findings	Comments
3.0	Design Assurance Methods For Level A and B Functions.	Analysis, Test Data	A/B	IEEE 7-4.3.2 does not specifically addresses the use of the design assurance methods based on functional failure path analysis listed in Appendix B of DO-254	

**4 IEEE 7-4.3.2 Deliverables and Aviation Process Equivalent**

The information in this section presents the deliverables from the Nuclear Standards on the left, followed by the Aviation Deliverable equivalent. The final right-most column discusses either the Objective Evidence or Process Equivalent within the Aviation processes, DO-254 and the system engineering information flow from processes such as ARP 4754 and ARP 4761. The DO-254 guidelines call for an iterative development with multiple re-entry points to assess the system and safety aspects. In addition DO-254 calls for a Hardware Accomplishment Summary and standards that are not listed in the IEEE 7-4.3.2 output provided. It is presumed that the PHAC and the Software Management Plan are reasonably equivalent and this report discusses that IEEE 7-4.3.2 does not call for a cert liaison process which includes a stated means of compliance.

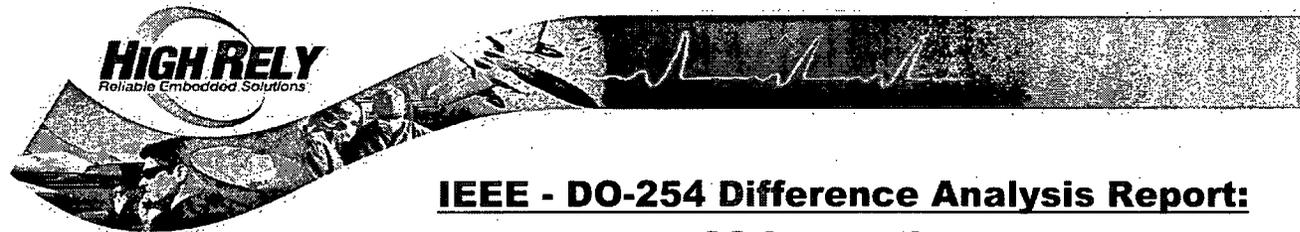


## IEEE - DO-254 Difference Analysis Report: CS Innovations

### 4.1 DO-254 Deliverables are defined as:

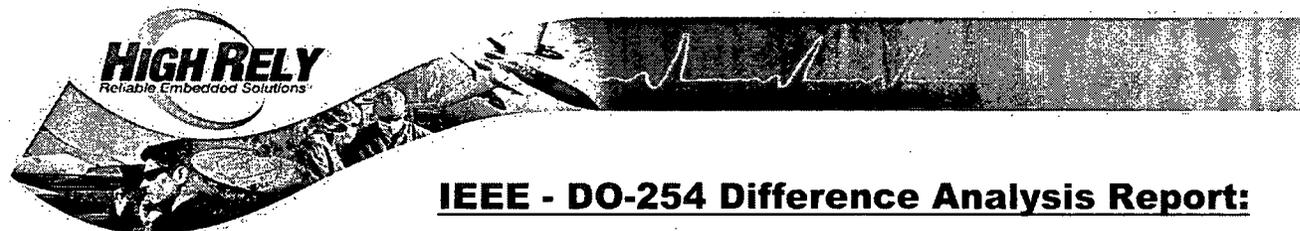
Hardware Life Cycle Data by Hardware Design Assurance Level and Configuration Control Code{TC "Table A-1 Hardware Life Cycle Data by Hardware Design Assurance Level and Configuration Control Code" \f t}

DO254 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
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



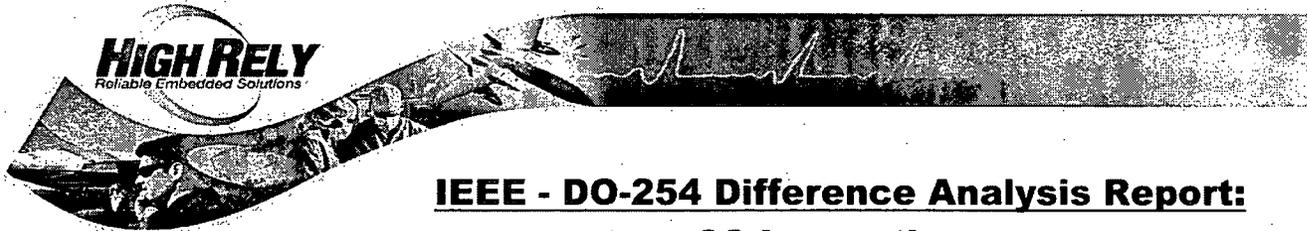
## IEEE - DO-254 Difference Analysis Report: CS Innovations

DO254 Data Section	Hardware Life Cycle Data <sup>①</sup>	Objectives <sup>②</sup>	Submit	Level A	Level B	Level C	Level D
10.3.2	Hardware Design Representation Data						
10.3.2.1	Conceptual Design Data <sup>③</sup>	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 <sup>③</sup>	5.3.1(1); 5.5.1(1)		HC1	HC1	HC1	HC1
10.4	Validation And Verification Data						
10.4.1	Hardware Traceability Data	6.1.1(1); 6.2.1(1,2)		HC2	HC2	HC2 <sup>⑥</sup>	HC2 <sup>⑥</sup>
10.4.2	Hardware Review and Analysis Procedures <sup>③</sup>	6.1.1(1,2); 6.2.1(1)		HC1	HC1	NA	NA
10.4.3	Hardware Review and Analysis Results <sup>③</sup>	6.1.1(1,2); 6.2.1(1)		HC2	HC2	HC2	HC2
10.4.4	Hardware Test Procedures <sup>③</sup>	6.1.1(1,2); 6.2.1(1)		HC1	HC1	HC2	HC2 <sup>⑦</sup>
10.4.5	Hardware Test Results <sup>③</sup>	6.1.1(1,2); 6.2.1(1)		HC2	HC2	HC2	HC2 <sup>⑦</sup>
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



## **IEEE - DO-254 Difference Analysis Report:** **CS Innovations**

- 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.
- 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 and/or presentation material.
- ⑤ If the applicant references this data item in required 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 required.



# **IEEE - DO-254 Difference Analysis Report: CS Innovations**

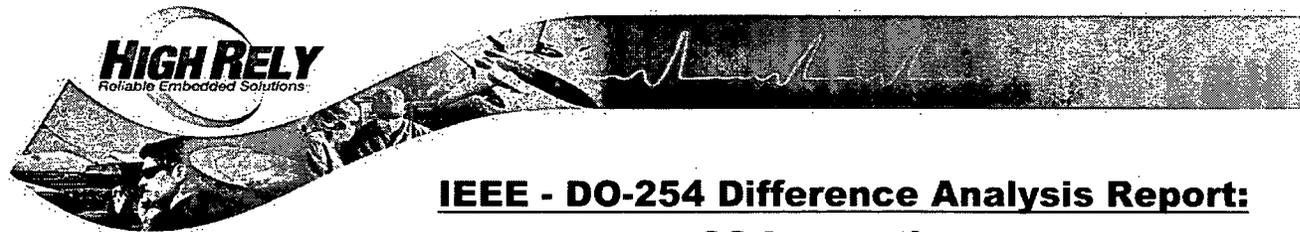


## **Required Certification Documentation**

- |  |   |
|--|---|
| 1. Plan for Hardware Aspects of Certification (PHAC) | 16. Installation Control Drawings             |
| 2. Hardware Design Plan                              | 17. Hardware/Software Interface Data          |
| 3. Hardware Validation Plan                          | 18. Hardware Traceability Data                |
| 4. Hardware Verification Plan (HVP)                  | 19. Hardware Review and Analysis Procedures   |
| 5. Hardware Configuration Management Plan            | 20. Hardware Review and Analysis Results      |
| 6. Hardware Process Assurance Plan                   | 21. Hardware Test Procedures                  |
| 7. Hardware Design Standards                         | 22. Hardware Test Results                     |
| 8. Requirements Standards                            | 23. Hardware Acceptance Test Criteria         |
| 9. Validation and Verification Standards             | 24. Problem Reports                           |
| 10. Hardware Archive Standards                       | 25. Hardware Configuration Management Records |
| 11. Hardware Requirements                            | 26. Hardware Process Assurance Records        |
| 12. Conceptual Design Data                           | 27. Hardware Accomplishment Summary (HAS)     |
| 13. Detailed Design Data                             |   |
| 14. Top-Level Drawing                                |   |
| 15. Assembly Drawings                                |   |

Copyright HighRelY 2005

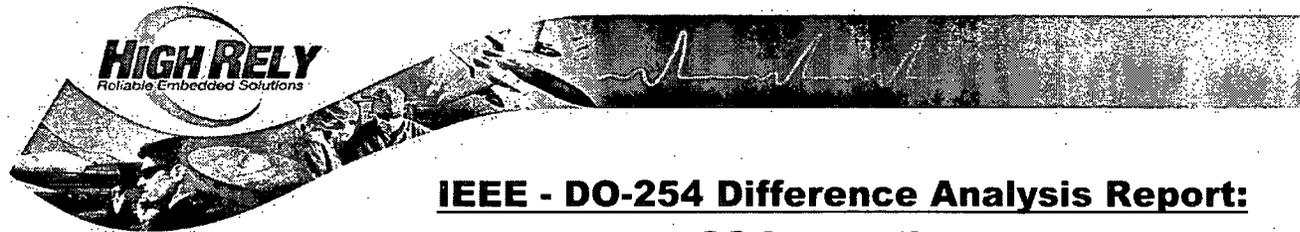
Slide 215



## IEEE - DO-254 Difference Analysis Report: CS Innovations

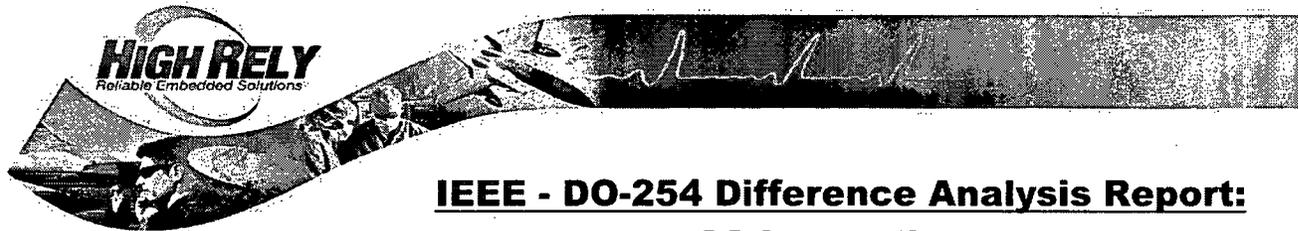
### 4.2 Deliverables of IEEE 7-4.3.2 Vs. Aviation Standards

Nuclear Deliverable	Aviation Deliverable			Objective Evidence or Process Equivalent
	SAE ARP 4754	SAE ARP 4761	RTCA DO-254	
<b>Planning Documentation:</b>				
Software Management Plan			PHAC	Plan for Hardware Aspects of Certification
Software Development Plan			HDP	Hardware Design Plan
Software Test Plan			HVP	Hardware Verification Plan
Software QA Plan			HPAP	Hardware Process Assurance Plan
Integration Plan			HDP	Hardware Design Plan
Installation Plan			HDP	Hardware Design Plan
Maintenance plan				Production Transition Process
Training plan				Production Transition Process
Operations Plan				Production Transition Process
Software Safety Plan		PSSA		Preliminary System Safety Assessment
Software V&V Plan			HVVP	Hardware Verification and Validation Plan
Software CM Plan			HCMP	Hardware Configuration Management Plan
			HRqtS	Hardware Requirement Standards
			HDesS	Hardware Design Standards
			HImpS	Hardware Implementation Standards
			HArchS	Hardware Archival Standards
<b>Design Specific Documentation:</b>				
Requirements Specifications	SSS		HRD	System Subsystem Specification
Requirement Traceability Matrix				System Information Flow Process/Traceability Data



**IEEE - DO-254 Difference Analysis Report:  
CS Innovations**

Nuclear Deliverable	Aviation Deliverable			Objective Evidence or Process Equivalent
	SAE ARP 4754	SAE ARP 4761	RTCA DO-254	
Design Specifications				System Information Flow Process
Major hardware component description and qualification				System Information Flow Process
Hardware & Software Architecture			HRD/HDD	Hardware Requirements or Design Data
Software Requirements Specification			HRD	Hardware Requirements Data
Software Design Description			HDD	Hardware Design Data (Conceptual and Detail)
Code Listings			HCI	Hardware Configuration Index/Top Level Drawing/Assembly Drawings
System Build Documentation			HECI	Hardware Environment Configuration Index Top Level Drawing/Assembly Drawings
Test Plans and Documentation			HVVP	Hardware Verification and Validation Procedures
Environmental test plans, procedures, and results			HVVP/HVVD	Environmental Configuration Hardware Verification and Validation Plan/Data/Results
Unit test plans, procedures, and results			HVVP/HVVD	Hardware Verification and Validation Plan/Data/Results
Integration test plans, procedures, and results			HVVP/HVVD	Hardware Verification and Validation Plan/Data/Results
Factory acceptance test plans, procedures, and results				Production Transition process
Site acceptance test plans, procedures, and results				Production Transition process
Installation test plans, procedures, and results			HVVP/HVVD	Hardware Verification and Validation Plan/Data/Results
<b>Analysis Documentation:</b>				
Requirements Safety Analysis		PSSA		Preliminary System Safety Assessment
Design Safety Analysis		PSSA		Preliminary System Safety Assessment
Code Safety Analysis		PSSA		Preliminary System Safety Assessment
Integration Safety Analysis		PSSA		Preliminary System Safety Assessment
Validation Safety Analysis		PSSA		Preliminary System Safety Assessment



**IEEE - DO-254 Difference Analysis Report:**  
**CS Innovations**

Nuclear Deliverable	Aviation Deliverable			Objective Evidence or Process Equivalent
	SAE ARP 4754	SAE ARP 4761	RTCA DO-254	
Installation Safety Analysis		SSA		System Safety Assessment
Change Safety Analysis		SSA		System Safety Assessment
Failure Modes and Effects Analysis (FMEA)		FMEA		Failure Mode and Effects Analysis
			HAS	Hardware Accomplishment Summary
<b>Verification and Validation (V&amp;V) Reports:</b>				
V&V Requirements Analysis Report			HVVR	Hardware Verification and Validation Results
V&V Design Analysis Report			HVVR	Hardware Verification and Validation Results
V&V Implementation Analysis & Test Report			HVVR	Hardware Verification and Validation Results
V&V Integration Analysis & Test Report			HVVR	Hardware Verification and Validation Results
V&V Validation & Test Report			HVVR	Hardware Verification and Validation Results
V&V Validation & Test Report			HVVR	Hardware Verification and Validation Results
V&V Change Report			HVVR	Hardware Verification and Validation Results
<b>Installation, Operations and Maintenance Documentation:</b>				
Operations Manuals				System Process
Maintenance Manuals				System Process
Training Manuals				System Process
Installation Configuration Tables				System Process
Spare Parts list				System Process
Repair Planning				System Process
System Retirements Plan				System Process